

**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

**CARRERA:
INGENIERÍA ELECTRÓNICA**

**Trabajo de titulación previo a la obtención del título de:
INGENIEROS ELECTRÓNICOS**

**TEMA:
DISEÑO DE UNA RED CON DMVPN SOBRE LA RED MPLS DE
PUNTONET**

**AUTORES:
CRISTIAN DARÍO IBAÑEZ MORENO
JUAN CARLOS PAZMIÑO QUIÑONEZ**

**TUTOR
JUAN CARLOS DOMÍNGUEZ AYALA**

Quito, agosto del 2020

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Cristian Darío Ibañez Moreno con documento de identificación N° 171842550-5 y Juan Carlos Pazmiño Quiñonez con documento de identificación N° 080458712-9, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: “DISEÑO DE UNA RED CON DMVPN SOBRE LA RED MPLS DE PUNTONET”, mismo que ha sido desarrollado para optar por el título de: Ingeniero Electrónico en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en digital a la Biblioteca de la Universidad Politécnica Salesiana.

Nombre: Cristian Darío Ibañez Moreno
Cédula: 171842550-5

Nombre: Juan Carlos Pazmiño Quiñonez
Cédula: 080458712-9

Fecha: Quito, agosto del 2020.

DECLARATORIA DE COAUTORIA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, “DISEÑO DE UNA RED CON DMVPN SOBRE LA RED MPLS DE PUNTONET”, realizado por Cristian Darío Ibañez Moreno y Juan Carlos Pazmiño Quiñonez, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, agosto del 2020



Juan Carlos Domínguez Ayala

Cédula de Identidad: 1713195590

DEDICATORIA

Dedico en primera instancia a Dios, por haberme dado la dicha de cumplir con este objetivo. A mi familia, especialmente a mi madre que con su amor, apoyo y consejos me dieron aquel impulso para no decaer a pesar de cada uno de los obstáculos que se presentaron en mi vida, pude continuar y sobrepasar cada adversidad. A mi hijo por ser aquella pequeña y a la vez gran inspiración que desde mi punto de vista la considero esencial y me dio el valor para seguir trabajando rigurosamente para culminar con éxito este, tan ansiado objetivo.

Juan Carlos Pazmiño Quiñonez

Dedicado a Dios y mi familia, por quienes me esfuerzo cada día por ser mejor persona y sin ellos nada de esto sería posible, su apoyo incondicional y oraciones han sido pilar en este proceso para la culminación de mi tesis y de mi carrera. Gracias a mi hermano que con su cariño ha logrado que mi vida tenga un caminar correcto.

Cristian Darío Ibañez Moreno

AGRADECIMIENTO

En primera instancia y ante todo quiero agradecer a Dios por haberme regalado la suficiente sabiduría para afrontar las diversas adversidades que se impusieron en mi camino tanto social como académicas, a la par por haber iluminado y guiado mi camino para que con ello logre culminar con éxito uno de mis objetivos planteados en la vida. A mi madre que, en paz, descanse que hizo todo lo necesario para dejarme la única y mejor herencia en mis manos, el estudio, por apoyarme en cada instancia de mi vida, sobre todo agradecer por sus consejos que me han convertido en un hombre de buenos valores. De la misma manera, agradecer a todos mis amigos y en especial a mi familia por su apoyo y preocupación en todo momento, ya que son aquellos pequeños detalles que perduran por siempre en la mente y corazón de una persona. Por último, quiero agradecer a mi tutor de tesis M.Sc. Juan Carlos Domínguez, por impartir sus conocimientos y guías académicas, la mismas que fueron de gran ayuda a lo largo de todo el proceso de titulación.

Juan Carlos Pazmiño Quiñonez

Gracias a Dios por el regalo de la vida, tu amor y bondad que me han permitido alcanzar este logro que tanto anhelaba. Y aun cuando caigo me levantas permitiéndome aprender de mis errores. A mi familia, que siempre ha estado apoyándome a lo largo de mis estudios y sobre todo a mi madre que con sus oraciones ha sabido cubrirme diariamente para que mis fuerzas no se desvanezcan. A mis amigos, que me han incentivado a continuar con mi carrera con sus palabras de aliento aun cuando estaba decido a retirarme. A la Empresa Puntonet, que me dio la oportunidad de trabajar y estudiar, que me facilitó los equipos para el diseño del proyecto de tesis y que me ha permitido crecer profesionalmente. A mi amigo y compañero de la empresa Ing. Víctor Araujo que me brindó su apoyo, ayuda y compartió sus conocimientos con gran predisposición. Por último, quiero agradecer a mi tutor de tesis M.Sc. Juan Carlos Domínguez, por compartirme sus conocimientos a lo largo de todo el proceso de titulación.

Cristian Darío Ibañez Moreno

ÍNDICE DE CONTENIDO

RESUMEN.....	x
ABSTRACT	xi
INTRODUCCIÓN.....	xii
ANTECEDENTES	1
1.1. Problema de Estudio.....	1
1.2. Justificación.....	1
1.3. Planteamiento del Problema	1
1.4. Objetivos.....	2
1.4.1. Objetivo General	2
1.4.2. Objetivos Específicos.....	2
1.5. Metodología de Diseño.....	3
CAPÍTULO 2.....	5
MARCO TEÓRICO	5
2.1. DMVPN.....	5
2.1.1. IPSEC.....	5
2.1.2. Protocolos con los que trabaja IPSEC.....	6
2.1.3. Módulos de funcionamiento del protocolo IPSEC.....	7
2.1.4. Protocolo ISAKMP	7
2.2. MPLS.....	9
2.2.1. Funcionamiento de una red MPLS.....	9
2.2.2. Etiquetas MPLS y niveles	10
2.3. Protocolo de enrutamiento OSPF	11
2.4. Protocolo de resolución del próximo salto (NHRP)	12
2.5. Protocolo VRRP	13
2.5.1. Funcionamiento de VRRP.....	14
2.6. Equipos MIKROTIK.....	14

CAPÍTULO 3.....	16
LÍNEA BASE DE LA INFRAESTRUCTURA DE LA RED DE PUNTONET S.A	
.....	16
3.1. Empresa PuntoNet S.A.....	16
3.2. Descripción de la infraestructura de la red provista por PuntoNet a escala nacional.....	17
3.2.1. La red MPLS de PuntoNet.....	17
3.3. Estructura de red de la sucursal sur PuntoNet.....	18
3.4. Estructura de red de la Matriz PuntoNet.....	18
3.4.1. Especificaciones de los equipos físicos de PuntoNet.....	19
CAPÍTULO 4.....	21
DISEÑO DE LA RED MDVPN SOBRE LA RED MPLS DE PUNTONET.....	21
4.1. Diseño.....	21
4.2. Diseño lógico.....	21
4.3. Direccionamiento IP.....	22
4.3.1. Direccionamiento de la red MPLS de PuntoNet.....	22
4.3.2. Direccionamiento para la conexión de la matriz a la sucursal sur	23
4.4. Diseño físico.....	24
4.5. Implementación y configuración.....	25
4.6. Configuración y prioridad para la interfaz LAN mediante el protocolo vrrp	25
4.7. Configuración DMVPN.....	27
4.7.1. Configuraciones router principal matriz	29
4.7.2. Configuración del protocolo IPSEC (matriz).....	29
4.7.3. Configuración del protocolo NHRP, OSPF y del túnel extremo a extremo (matriz)	33
4.7.4. Configuraciones router sucursal.....	36
4.7.5. Configuración IPSEC Backup.....	36

4.7.6. Configuración del protocolo NHRP, OSPF y del túnel extremo a extremo (sucursal).....	37
CAPÍTULO 5.....	40
PRUEBAS Y ANÁLISIS DE CONECTIVIDAD DE LA RED DMVPN	40
5.1. Red DMVPN	40
5.2. Prueba y análisis de comunicación equipos cisco matriz y sucursal	40
5.2.1. Tabla DMVPN matriz y sucursal	40
5.2.2. Prueba de comunicación desde la matriz hacia la sucursal.....	42
5.2.3. Tabla IPSEC	43
5.2.4. Tabla ISAKMP.....	45
5.3. Prueba y análisis equipo Mikrotik backup, sucursal	48
5.3.1. Prueba de comunicación desde la sucursal hacia la matriz.....	49
5.4. Validación de retardos en el envío de paquetes Matriz-Sucursal Sur	50
5.5. Análisis de costos para la viabilidad y rentabilidad del proyecto	57
5.5.1. CÁLCULO DEL VALOR PRESENTE NETO (VPN)	58
5.5.2. Cálculo de la tasa interna de retorno (TIR)	61
CONCLUSIONES.....	63
RECOMENDACIONES.....	64
BIBLIOGRAFÍA.....	65
ANEXOS	1

ÍNDICE DE FIGURAS

figura 1. Funcionamiento de IPSec vinculado con una VPN.....	6
figura 2. Niveles para el encapsulamiento de etiquetado del MPLS.....	10
figura 3. Proceso de etiquetado del MPLS	11
figura 4. explicación del funcionamiento del protocolo OSPF basado en el algoritmo Dijkstra.....	11
figura 5. Topología del funcionamiento del protocolo VRRP	14
figura 6. Infraestructura de la red MPLS DE PUNTONET S.A.	17
figura 7. Diagrama físico de red Matriz-Sucursal Sur de PuntoNet.	20
figura 8. Topología física	25
figura 9. configuración del protocolo vrrp en la Sucursal, equipo cisco.....	26
figura 10. tabla del protocolo vrrp.....	26
figura 11. Configuración para asignar la prioridad y tiempo de conmutación al protocolo VRRP en el equipo Mikrotik, backup.....	27
figura 12. Configuración protocolo VRRP equipo Backup	27
figura 13. configuración del protocolo IPSEC equipos CISCO.....	30
figura 14. Comando para la configuración del protocolo IPSEC.....	30
figura 15. Comando para la configuración del protocolo IPSEC.....	30
figura 16. Comando para la configuración del protocolo IPSEC.....	31
figura 17. Comando para la configuración del protocolo IPSEC.....	31
figura 18. configuración del protocolo IPSEC en equipos CISCOS.....	32
figura 19. Comando para la configuración del protocolo IPSEC.....	32
figura 20. configuración de transformación de IPSEC profile y protección del túnel.....	33
figura 21. Comando para la configuración del protocolo IPSEC.....	33
figura 22. configuración de los túneles dinámicos mediante el protocolo mGRE.....	34
figura 23. Configuración del túnel mediante el protocolo NHRP (Matriz)	35
figura 24. Tabla del protocolo NHRP	35
figura 25. Funcionamiento del protocolo IPSEC en el equipo Mikrotik Backup	36
figura 26. Tabla de configuración del protocolo NHRP y los túneles (sucursal)	37
figura 27. Tabla configuración del protocolo OSPF (sucursal)	38
figura 28. configuración del protocolo OSPF en el router Mikrotik backup	39
figura 29. tabla DMVPN de la matriz	41
figura 30. figura 23. tabla DMVPN de la sucursal.....	41

figura 31. tabla de detalles del protocolo NHRP.....	42
figura 32. Tabla de enrutamiento IP.....	42
figura 33. ping desde la matriz hacia la IP física del Backup e IP virtual (LAN) de la sucursal.....	43
figura 34. tabla IPSec Matriz, conexiones activas de paquetes cifrados.....	43
figura 35. tabla IPSec Matriz	45
figura 36. Tabla del protocolo ISAKMP Matriz	45
figura 37. Tabla del protocolo ISAKMP Sucursal	46
figura 38. Tabla del sistema de seguridad de encriptación IKE, IPSEC.....	47
figura 39. Backup Down	48
figura 40. Backup up.....	48
figura 41. tabla de enrutamiento de la sucursal.....	49
figura 42. Ping desde la sucursal a la IP virtual (LAN) de la Matriz.....	50
figura 43. Ping desde la sucursal a la WAN de la Matriz	50
figura 44. Validación en el envío de paquetes desde la matriz hacia la sucursal bajo una configuración simple	51
figura 45. Validación en el envío de paquetes desde la sucursal hacia la matriz bajo una configuración simple	51
figura 46. Validación en el envío de paquetes desde la matriz hacia la sucursal bajo una red con DMVPN.....	52
figura 47. Validación en el envío de paquetes desde la sucursal hacia la matriz bajo una red con DMVPN.....	52
figura 48. Demostración grafica de una red con VPN simple vs DMVPN.....	53
figura 49. Validación en el envío de paquetes desde equipo matriz hacia el equipo Backup prueba 1.....	55
figura 50. Validación en el envío de paquetes desde el equipo Backup hacia el equipo matriz prueba 2.....	56
figura 51. Fórmula para el cálculo del valor presente neto (VPN)	58
figura 52. Descripción de los flujos del proyecto dentro de un periodo determinado	59
figura 53. Fórmula para el cálculo de la tasa interna de retorno (TIR).....	61

ÍNDICE DE TABLAS

Tabla 1. Direccionamiento y asignación de puertos para red MPLS del equipo R1 de PuntoNet.....	22
Tabla 2. Direccionamiento y asignación de puertos para red MPLS del equipo R2 de PuntoNet.....	22
Tabla 3. Direccionamiento y asignación de puertos para red MPLS del equipo R4 de PuntoNet.....	22
Tabla 4. Direccionamiento IP y asignación de puerto para la conexión a la sucursal mediante el router R2.....	23
Tabla 5. Direccionamiento IP y asignación de puerto para la conexión a la matriz mediante router R1.....	23
Tabla 6. Direccionamiento IP y asignación de puerto para la conexión al backup mediante router R4.....	23
Tabla 7. Descripción de equipos físicos.....	24
Tabla 8. Validación de retardos en el envío de paquetes Matriz-Sucursal	53
Tabla 9. Validación de retardo en el envío de paquetes Matriz-Backup	56
Tabla 10. Costo de equipos y materiales implementados en el proyecto.....	58
Tabla 11. Valores provistos por la empresa Puntonet para el cálculo correspondiente del VPN.....	59
Tabla 12. Descripción económica de la rentabilidad y viabilidad el proyecto	62

RESUMEN

El presente proyecto tiene como finalidad el diseño de la red DMVPN sobre la red MPLS de la empresa Puntonet, con la cual se evitará demoras en la entrega de cualquier tipo de datos requeridos, además proporcionará redundancia para garantizar la disponibilidad del servicio, esta propuesta es viable debido a que se trata de una red de tamaño medio, la misma que va a estar basada en la red MPLS de Puntonet, lo que permitirá aprovechar al máximo la capacidad del switch. Se explicará el funcionamiento, características y configuración de los protocolos de enrutamiento, de encriptación y desencriptación de paquetes y de seguridad para la comunicación matriz-sucursal, todo esto estará basado bajo una metodología brevemente explicada de diseño la cual ayudará a estructurar de manera técnica la línea base del proyecto y con ello poder finalizar de una manera adecuada cada uno de los objetivos planteados y poder plasmar los mismos en un escenario idóneo o como tal diseño físico el cual cumpla con todas las expectativas de PuntoNet. Por último, se llevará a cabo las pruebas de enrutamiento de la red las mismas que serán de gran aporte para demostrar y verificar el diseño de la red con DMVPN, así como comprobar las buenas prácticas de configuración de equipos reales, además del correcto análisis financiero de la red diseñada el cual aportará a determinar si el proyecto propuesto es tanto viable como rentable para PuntoNet.

ABSTRACT

The purpose of this project is the design of the DMVPN network over the MPLS network of the company Puntonet, which will avoid delays in the delivery of any type of data required, in addition will provide redundancy to guarantee the availability of the service, this proposal is feasible because it is a medium-sized network, the same that will be based on the MPLS network of Puntonet, which will allow you to take full advantage of the switch's capacity. It will explain the operation, characteristics and configuration of the routing, encryption and packet decryption and security protocols for matrix-branch communication, all this will be based under a briefly explained design methodology which will help to technically structure the project baseline and thereby be able to adequately complete each of the objectives set out and be able to translate the same in an ideal scenario or as such a physical design which is able to correct in an appropriate way Meet all PuntoNet expectations. Finally, the network routing tests will be carried out that will be of great contribution to demonstrate and verify the design of the network with DMVPN, as well as check the best practices of configuration of real equipment, as well as the correct financial analysis of the designed network that will help determine whether the proposed project is both feasible and cost-effective for PuntoNet.

INTRODUCCIÓN

El presente proyecto trata del diseño de una red mediante el cual tiene como finalidad mejorar el envío de paquetes de un extremo a otro con menor latencia, así como el poder brindar redundancia a la red en el caso de que llegase a existir una falencia en la misma, además se añade una alta gama de seguridad mediante algoritmos de cifrado y descifrado, los cuales proporcionarían la seguridad necesaria para la red, este trabajo se fragmenta como tal en 5 capítulos.

En el capítulo 1, se especificarán los objetivos tanto general como específicos, así como el planteamiento del problema y su posterior justificación, además se dispone de una metodología de diseño para estructurar la línea base del proyecto el cual con lleve a la correcta configuración de la red DMVPN. En cambio, en el capítulo 2, se darán a conocer las funcionalidades de los términos que se aplicarán en el proyecto, tales como, significado, estructura de funcionalidad, protocolos, etc.

En el capítulo 3, se explicará la línea base del proyecto, es decir, se dará a conocer a breve rasgo, la tecnología que conserva PuntoNet, así como su topología, equipos implementados, empresas a las que ofrece su servicio, su estructura de red MPLS, etc.

Mientras tanto en el capítulo 4, se explicará el diseño tanto lógico como físico el cual va a ser implementado, así como su respectivo direccionamiento IP, en este capítulo también expondremos la configuración de cada uno de los protocolos, a implementar tales como; OSPF, IPSEC, ISAKMP, VRRP y NHRP, también se mostrará la configuración de algoritmos de encriptación de claves como; 3DES, AES entre otros. En el capítulo 5 se dará paso a las pruebas de enrutamiento de la red para verificar cada una de las configuraciones previas, así como la demostración y verificación del funcionamiento DMVPN y mGRE dentro de la red, la conexión de pares mediante túnel, además del enlace secundario para brindar redundancia en el caso de que exista un fallo en la comunicación del router principal de la sucursal sur. Se hará el análisis económico de costos e inversiones para determinar si el proyecto es viable y rentable para PuntoNet.

CAPÍTULO 1

ANTECEDENTES

1.1. PROBLEMA DE ESTUDIO

Puntonet S.A con su matriz en Quito cubre varias ciudades como son: Guayaquil, Cuenca, Santo Domingo, Ambato entre otras brindando sus servicios de enlace empresariales.

Puntonet S.A ha incrementado el crecimiento de sus usuarios generando una gran demanda en el tráfico provocando que el ancho de banda proporcionado por la matriz hacia las distintas sucursal sea insuficiente por lo que se evidencia una saturación en el canal por ende se reflejará ante los usuarios como retardos e intermitencias que afectan los tiempos de respuestas en las peticiones remotas que realizan los usuarios finales en sus aplicaciones provocando demoras en las transacciones y en la gestión de los procesos que se reflejaran como pérdidas económicas a la empresa.

1.2. JUSTIFICACIÓN

Realizar el diseño de una red DMVPN sobre la red MPLS de Puntonet permitirá mantener una conexión continua a los usuarios empresariales pertenecientes al servicio de internet de la empresa PuntoNet, debido a que se tendrá una mejora en el desempeño y disponibilidad de la red, disminuyendo la latencia de la red y garantizando el tráfico de la información de manera segura evidenciando una agilización en la ejecución de trabajos, facturaciones y procesos asociados a la matriz y sus sucursales lo que con lleva una mejora económica para la empresa.

1.3. PLANTEAMIENTO DEL PROBLEMA

Al generarse un porcentaje considerable de procesamiento del tráfico en una red de la empresa debido al excesivo crecimiento por demanda de usuarios tanto a nivel residencial, como comercial y empresarial, es incuestionable que el medio de transmisión por donde viajan las señales portadoras de información presentará colapso, por lo tanto la demanda de usuarios divisarán retardos temporales o a su vez latencia lo cual afecta directamente a los tiempos de respuesta en el cual se transmiten los datos entre la Matriz principal de la empresa y las sucursales asociadas a la misma,

provocando una mayor latencia ya que los usuarios realizan peticiones de conexión remota a los servidores para conectarse o a su vez transmitir información de un extremo a otro, todos estos inconvenientes al final generan retardos temporales en las gestión con el cliente final provocando la indisponibilidad del enlace, lo cual significa pérdidas tanto de información como pérdidas económicas.

¿Será capaz el nuevo diseño de red la solución para corregir el tráfico, evitar retardos temporales y mantener la redundancia en la transmisión de datos de la Empresa Puntonet y cada una de sus Sucursal para una gestión modular de la arquitectura de red existente permitiendo una mayor flexibilidad, escalabilidad y seguridad de servicio?

1.4. OBJETIVOS

1.4.1. Objetivo General

Diseñar una red tolerante a fallos mediante DMVPN sobre la red MPLS de Puntonet para la redundancia de datos y gestión modular de la arquitectura de red existente permitiendo una mayor flexibilidad, escalabilidad y seguridad de servicio.

1.4.2. Objetivos Específicos

- Determinar la línea base de la red actual para la identificación de las limitaciones técnicas y empresariales de Puntonet.
- Diseñar la red para la redundancia de datos en las sucursales pertenecientes a Puntonet para el cumplimiento de flexibilidad y escalabilidad dentro de la entidad empresarial mediante cada una de las fases de la metodología PPDIIO.
- Implementar un prototipo para la validación de retardos en un punto estratégico de la topología.
- Analizar los costos de la implementación de la red para que se conozca la viabilidad del proyecto.

1.5. METODOLOGÍA DE DISEÑO

Para el posterior diseño se hace uso de dos métodos investigativos los cuales tratan del enfoque sistemático y técnico de la empresa PuntoNet, los cuales son los siguientes:

- **Método inductivo:** Se llevará a cabo un enfoque sistemático de cada uno de sus parámetros actuales realizando un testeo diario con el cual se pueda determinar la línea base de la red actual la misma que nos llevara a saber a nivel del proyecto cuales son las limitaciones técnicas.
- **Método analítico:** El diseño de una nueva red el cual cumpla con todos los requerimientos tales como flexibilidad, escalabilidad y seguridad de la red, con el cual se logrará realizar un contraste de la red actual y la red diseñada donde se podrá visualizar las mejoras, así como el cumplimiento de cada uno de los requerimientos de la red, con el cual se podrá determinar la viabilidad del proyecto en la entidad empresarial.

Para plasmar estos métodos de investigación y poder obtener una estructura tanto viable como a su vez funcional, nos basaremos en el método de diseño PPDIOO (preparación, planificación, diseño, implementación y optimización), todo este proceso será de gran ayuda para entender el funcionamiento y configuración de la tecnología DMVPN, la misma que a su final proporcionará una red con alta disponibilidad, integridad, escalabilidad y sobre todo que sea rentable para la empresa PuntoNet.

- **Preparación:** En la fase de preparación se realizará una visita técnica al lugar de realización del proyecto, tomando en cuenta ciertos parámetros a nivel empresarial, siendo esto la línea base del proyecto, en el cual nos enfocaremos en mitigar información relevante y de esta manera poder deducir que es lo que se necesita para el diseño de la red DMVPN.
- **Planificación:** En esta fase hacemos uso o en definitiva nos basaremos bajo el método analítico ya explicado con anterioridad, en el cual se describe que en el lugar donde se va a realizar el proyecto ya cuenta con una red y mediante el cual

analizaremos la finalidad de por qué PuntoNet requiere implementar una nueva red, esta fase será de gran ayuda más adelante ya que se podrá visualizar un contraste de la red actual y diseñada en la cual se exhibirá las mejoras las cuales incluyen un alto nivel de disponibilidad, integridad y escalabilidad.

- **Diseño:** En esta fase se debe diseñar la red propuesta la cual logre a gran escala cumplir con las expectativas de la empresa, es decir, que cumpla con una excelente comunicación matriz-sucursal, disponibilidad, integridad y sobre todo seguridad al momento de enviar y recibir información de extremo a extremo, así como la distribución correcta del direccionamiento IP en cada uno de los equipos involucrados en la topología diseñada.
- **Implementación:** Una vez determinado el diseño, mediante esta fase se procede a la configuración de cada uno de los equipos para que cumplan con su rol respectivo de matriz y sucursal, así como establecer redundancia de datos si es que en algún momento llegase a existir algún inconveniente en la red además de la configuración de protocolos y algoritmos de encriptación y desencriptación de paquetes para mayor seguridad.
- **Operación:** En esta fase se realiza todas las pruebas necesarias para comprobar el funcionamiento educado de la red diseñada, es decir, nos enfocaremos en la conectividad extremo-extremo, que los protocolos de seguridad estén operando correctamente sobre la red, además en dicha fase podremos analizar si la red propuesta cumple con los requerimientos de disponibilidad, integridad y escalabilidad que pretende PuntoNet.
- **Optimización:** En esta fase se llevará a cabo una evaluación técnica del funcionamiento de la red diseñada, así como la implementación de más equipos o en su defecto para el mantenimiento preventivo y correctivo de los equipos, además si la empresa lo requiere se darán propuestas para la configuración de routers para el cambio y direcciones IP acorde al requerimiento que la red diseñada sea escalable, así como procesos para evitar el colapso o interrupción en el envío de datos de matriz a sucursal.

CAPÍTULO 2

MARCO TEÓRICO

2.1. DMVPN

El termino DMVPN hace la referencia a caminos múltiples dinámicos basados en una VPN, en otras palabras, se trata básicamente de un protocolo de seguridad de CISCO el cual es útil para trabajar en la elaboración o a su vez en crear VPN seguras, cabe destacar que las DMVPN creadas establecen una conexión dinámica justo en el momento que se solicite el envío de información matriz-sucursal o sucursal-sucursal, (Barrientos Sevilla & Ariganello, 2015)

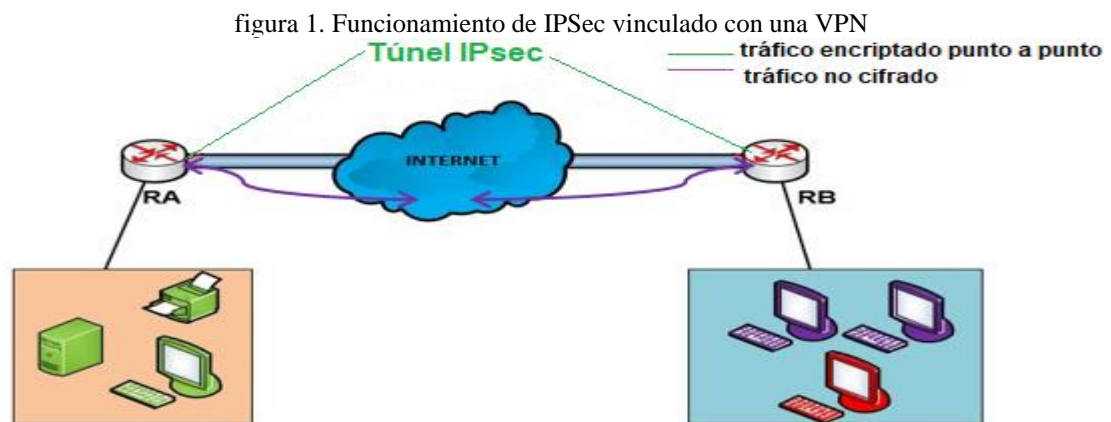
La tecnología propuesta por CISCO, DMVPN brinda además de una excelente conectividad también en la red en donde se la esté empleando sea dinámica por lo tanto el uso de este protocolo de seguridad no genera algún problema al momento de añadir o en definitiva de suprimir un túnel, es decir, no genera un nivel alto de complejidad en cambios de configuración. Cabe destacar que DMVPN está pre establecido una configuración desde un principio con la única finalidad de trabajar dentro de una topología de conectividad matriz a sucursal, haciendo uso de esta red en primera instancia los túneles entre matriz a sucursales y sucursal a sucursal originarios se puede adquirir o hablando de una forma un poco técnica se logra construir una conexión dinámica, (Barrientos Sevilla & Ariganello, 2015)

Para que DMVPN funcione es necesario configurar el protocolo mGRE, que como su nombre lo indica permite el soporte de múltiples túneles, a niveles de diseño mGRE puede ser implementado en dos entornos distintos, los cuales pueden ser comunicación sucursal(spoke)-sucursal(spoke) o también matriz(hub)-sucursal(spoke) siendo este último empleado para nuestro diseño de la red DMVPN. Además, el protocolo mGRE, requiere el uso exclusivo del protocolo NHRP para la formación de túneles dinámicos. (Barrientos Sevilla & Ariganello, 2015)

2.1.1. IPSEC

Por sus siglas en ingles IPSEC se lo conoce como IP Security, como su nombre lo indica fue diseñado para brindar una mayor seguridad a las redes IP, es decir, al

protocolo IP, como se puede apreciar en la figura 1, dispone un nivel alto de seguridad al momento de crear VPN's, sobre el internet, mediante un túnel. (García, 2015)



Elaborado por: Cristian Ibañez, Juan Pazmiño

2.1.2. Protocolos con los que trabaja IPSEC

Cabe destacar la buena labor que presenta IPSec al momento de proporcionar altos niveles de seguridad en las redes IP, adicional a esto, brinda excelentes estados tanto de integridad como confidencialidad y a su vez autenticidad, todo esto resumido como protección de envío de información de un usuario a otro. (García, 2015)

Todo aquel proceso de protección lo lleva a cabo mediante los siguientes protocolos:

- **Authentication Header (AH, RFC 2402):** Este protocolo como su nombre lo indica, brinda autenticación y a la par integridad de información referente al remitente adicional a esto se sujeta a la seguridad contra el reenvío de datos. (García, 2015)
- **Encapsulating Security Payload (ESP, RFC 2406):** Este protocolo trabaja en conjunto con el protocolo Authentication Header (AH), explicado en el ítem anterior, el protocolo ESP, brinda cargos de autenticación, integridad y a su vez protección contra el reenvío, referentes al remitente adicional a esto también tiene como función el de cifrar la información enviada para que de una u otra manera garantice al usuario o varios usuarios confidencialidad. (García, 2015)

- **Security Association (SA):** Este protocolo tiene como única finalidad el enunciar tanto el conjunto global de claves y a su vez políticas de seguridad para poder crear una comunicación estable, cabe mencionar que para poder ejecutar este protocolo con éxito es necesario conocer una dirección IP de destino, un identificador de protocolo y en definitiva un valor determinado como Security Parameter Index (SPI). (García, 2015)

2.1.3. Módulos de funcionamiento del protocolo IPSEC

Existen dos modos de funcionamiento del cual se apoya el protocolo security (IPSEC), los cuales son los siguientes:

- **Modo túnel:** Este modo de funcionamiento este acoplado o a su vez trabaja en conjunto con una red virtual privada (VPN), lo que indica que brinda aquella conexión estable y segura dando labor al cifrado de paquetes IP entre routers, cabe destacar que dicha función de seguridad admite la creación de túneles VPN (García, 2015)
- **Modo transporte:** En cambio, este modo da la opción de establecer una conexión segura, pero en esta ocasión los routers están de extremo a extremo, debido a que en este modo no se cifra la cabecera de los paquetes IP. (García, 2015)

2.1.4. Protocolo ISAKMP

ISAKMP por sus siglas en inglés significa Internet Security Association and Key Management Protocol, esta tecnología de red tiene como finalidad la creación, intercambio y gestión autónoma tanto de claves como de autenticaciones. (Maillo Fernandez, 2017)

Este protocolo además de poder gestionar claves también tiene la funcionalidad de mitigar cualquier amenaza que quiera irrumpir en la red, además define los procedimientos, así como la estructura de datos para determinar, modificar, gestionar y eliminar las SA (Security Association). Dentro de ISAKMP opera IKE que a su vez es parte esencial del sistema de administración de claves a nivel del internet. (Maillo Fernandez, 2017)

IKE opera mediante la sujeción de dos fases tales como:

- **Fase 1 de negociación IKE:** Esta fase se encarga de la autenticación, tomando todas las medidas precautelares necesarias para establecer un canal seguro de comunicación punto a punto entre los extremos de la red. (Maillo Fernandez, 2017)
- **Fase 2 de negociación IKE:** Tiene como finalidad, constituir y restablecer las SA (security association) que necesita el túnel de IPSec. (Maillo Fernandez, 2017)

2.1.5. Funcionamiento de IPSEC basado en ISAKMP e IKE

Como tal el protocolo IPSEC brinda una alta gama de seguridad a nivel de red, siendo optimo y muy útil en el mundo de las redes, lo que a su vez lo convierte en un sistema muy complejo de configurar, dicho protocolo opera en orden de la siguiente manera:

- Los equipos que estén al extremo de la red deben de enviar un paquete de datos estableciendo así de esta manera tráfico, y poder evidenciar la DMVPN. (Maillo Fernandez, 2017)
- Una vez establecida la conexión extrema, extremo entre ambos equipos involucrados en la topología, se ejecuta la fase1 de negociación IKE llevando a cabo la autenticación de la comunicación de los equipos ubicados a los extremos. (Maillo Fernandez, 2017)
- Mediante la fase 2 de negociación IKE, se genera la SA (Security Association), la misma que se implementara sobre el túnel IPSec. (Maillo Fernandez, 2017)
- Se lleva a cabo la transmisión de información, estos datos enviados son a su vez encriptados mediante el algoritmo implementado y acordado en la SA (Security Association), que en este caso se hizo uso del sistema 3DES. (Maillo Fernandez, 2017)

2.2. MPLS

MPLS por sus siglas en ingles se refiere a Multiprotocol label switching, trata de un sistema de mecanismos de enrutamiento de tráfico dentro del entorno de una red, cabe destacar que la información que se transmite de un nodo de red hacia otro provee determinadas aplicaciones que involucran redes privadas virtuales tales como VPN, así como ingeniería de tráfico y por último calidad de servicio. (Dordoigne, 2020)

2.2.1. Funcionamiento de una red MPLS

Cabe destacar que una red MPLS brinda aquel servicio o se puede decir soporte a cada nodo, en el cual están involucrados tanto un switch como router además fija etiquetas a cada uno de los elementos determinados en la tabla de ruteo y notifica a cada uno de sus nodos vecinos. Cabe tener en cuenta que una red MPLS basa su funcionamiento mediante el etiquetado de un paquete, es decir, cuando una PC 1 envía información a la PC2 mediante una red MPLS, este debe de seguir un camino: (Dordoigne, 2020)

- El paquete de datos enviado desde la PC1 llega hacia un enrutador IP común este sirve de intermediario para poder llegar al enrutador MPLS determinado como punto extremo de ingreso.
- Se procede al análisis del destino del paquete de datos enviado por la PC1.
- Se denomina una FEC, cabe tener en cuenta que cada FEC tiene un determinado camino ya establecido por la red MPLS el mismo que opera de forma independiente tanto de un switch como de un router.
- Para tener noción de que etiqueta asignarle al paquete de datos se procede a la comparación con las demás etiquetas establecidas en la tabla de enrutamiento las mismas que se van fijando desde la dirección destino y origen por medio de información enviado por switches o router.
- Una vez establecida o determinada la tabla de enrutamiento al paquete se le asigna una etiqueta la misma que ira cambiando o variando en cada switch o Router MPLS el mismo que solo llega revisando dicha etiqueta.

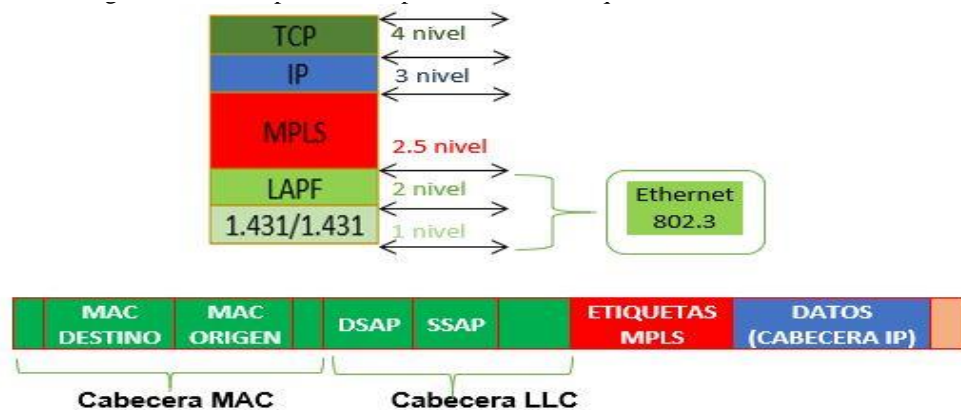
2.2.2. Etiquetas MPLS y niveles

Cabe destacar que las etiquetas tienen solamente un significado a nivel local de redes, por ejemplo:

- Son aquellas en las cuales tienen una postura relevante o significativa para el enlace entre dos LSR.
- Se define la ruta mediante la red MPLS

La red MPLS tiene soporte para dominios o en definitiva niveles como se puede apreciar en la figura 2, está compuesto por 4 niveles de distribución en el cual los niveles correspondientes a TCP e IP hacen referencia a los segmentos y datagramas de la cabecera IP de datos, mientras que el nivel MPLS es el etiquetado de datos este se ubica en el nivel 2.5 y por ultimo los niveles de Ethernet hacen simplemente referencia a la cabecera MAC y LLC. (Dordoigne, 2020)

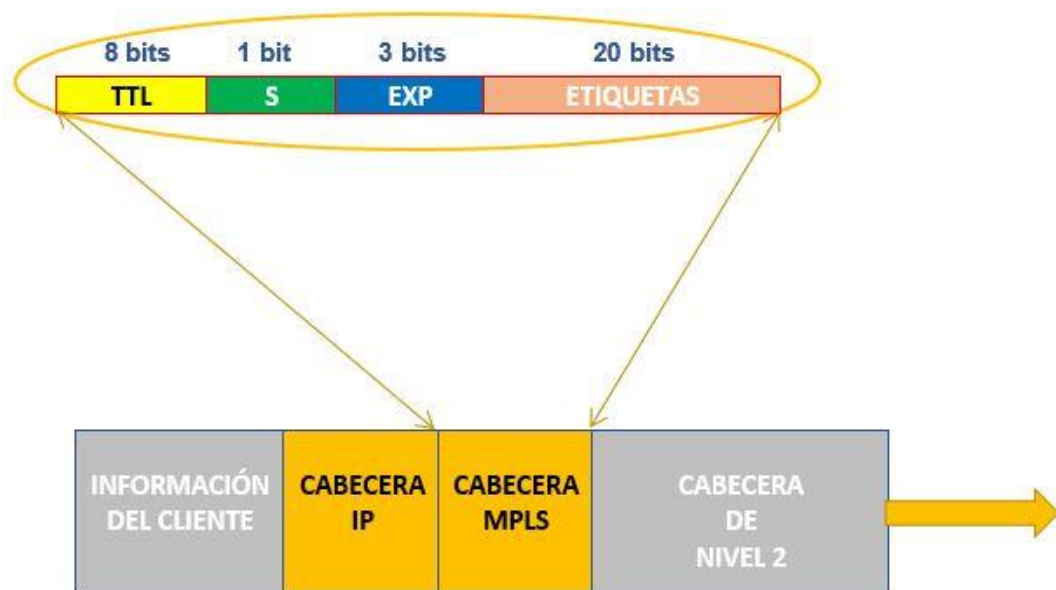
figura 2. Niveles para el encapsulamiento de etiquetado del MPLS



Elaborado por: Cristian Ibañez y Juan Pazmiño

A este proceso también se lo conoce como encapsulamiento de etiqueta para MPLS con el cual se puede tomar definiciones específicas para más de una red virtual para uno o varios paquetes de datos, para esto como se indica en la figura 3, la red MPLS toma en cuenta una pila de etiquetas en la cabecera de los paquetes. (Dordoigne, 2020)

figura 3. Proceso de etiquetado del MPLS

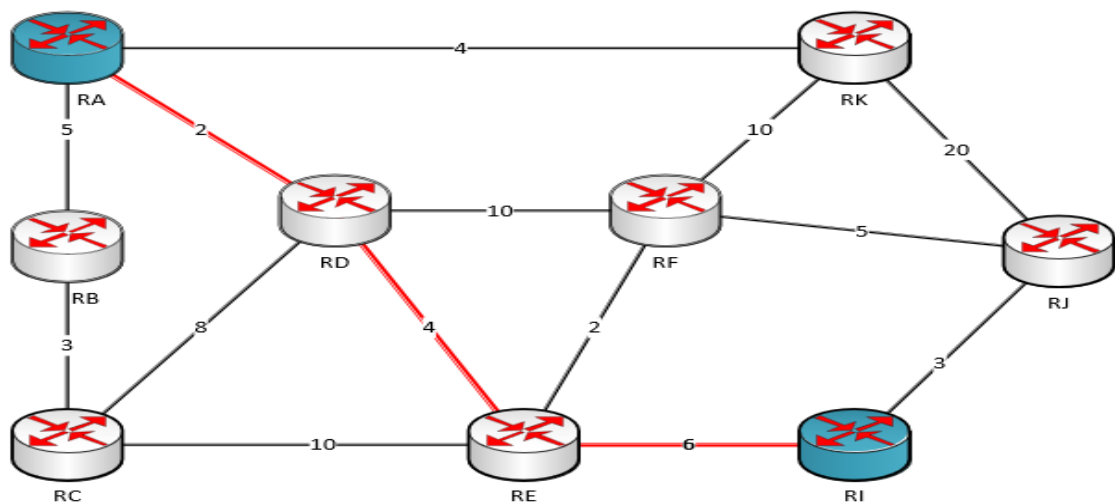


Elaborado por: Cristian Ibañez y Juan Pazmiño

2.3. PROTOCOLO DE ENRUTAMIENTO OSPF

OSPF, también denominado por sus siglas en español como paso por el camino más corto, en primera instancia, es un protocolo de enrutamiento o a su vez de encaminamiento haciendo referencia al estado de enlace, como se puede apreciar en la figura 4, este protocolo se basa en el algoritmo de Dijkstra, brindando una mayor rapidez en la convergencia y autenticación de información para el envío de datos. (Barrientos Sevilla & Ariganello, 2015)

figura 4. explicación del funcionamiento del protocolo OSPF basado en el algoritmo Dijkstra



elaborado por: Cristian Ibañez, Juan Carlos Pazmiño

Cabe destacar que OSPF hace uso del protocolo de Routing del estado de enlace de una manera distinta por no decir opuesta al protocolo RIP, ya que este último para enlazar o enrutar hace uso del vector distancia, en cambio OSPF se basa por el camino más corto. (Barrientos Sevilla & Ariganello, 2015)

Para un óptimo funcionamiento en el estado de enlace OSPF hace referencia de los siguientes protocolos:

- **Hello:** Este protocolo, brinda a los equipos involucrados en la topología como tal a los routers, de una u otra manera verificar la conexión existente con sus vecinos, el estado de conexión de este protocolo mediante sus paquetes hello se sujetan a múltiple información tales como; identificador de cada uno de los equipos, intervalo entre cada uno de los paquetes hello, dato específico de su estado de enrutamiento, prioridad y ubicación del router y próximos vecinos. (Barrientos Sevilla & Ariganello, 2015)
- **Inundación:** Este protocolo es más para analizar y detectar algún cambio en la red, es decir, este mantiene en el router descripción del estado de conexión en la topología y a su vez envía las actualizaciones de su información de estado a todos sus vecinos. (Barrientos Sevilla & Ariganello, 2015)
- **Intercambio:** Este protocolo es una técnica que brinda a cada uno de los routers configurados con dicha tecnología el poder intercambiar información a nivel de topología. (Barrientos Sevilla & Ariganello, 2015)

2.4. PROTOCOLO DE RESOLUCIÓN DEL PRÓXIMO SALTO (NHRP)

Es aquel protocolo que se encarga de brindar un alto margen de eficiencia con respecto al tráfico o envío de datos de la red especialmente o en definitiva enfocado a topologías tipo NBMA. (Ortiz Palomino & López Cadena, 2019)

NHRP por sus siglas en inglés se trata del next hop resolution protocol, el cual tiene como finalidad el aprender de una manera dinámica las direcciones que en sí forman parte de la topología, proporcionando a su vez que los routers se comuniquen o transfieran datos directamente, desistiendo de la opción de solicitar tráfico mediante

un salto intermedio. A breves rasgos el protocolo NHRP está basado en el sistema cliente, servidor en donde el cliente (NHC) se encarga de consultar todas y cada una de las direcciones IP de los demás clientes pertenecientes al servidor (NHS) brindando la opción de que todos los equipos se comuniquen directamente entre sí además este protocolo puede inspeccionar su propia dirección IP con el de servidor (NHS) que a su vez lleva a cabo una mitigación de todos los radios registrados en la red. servidor (NHS). Para el envío de paquetes referentes al NHRP, este debe incluir en su estructura las direcciones IP tanto pública, de origen, así como las direcciones de protocolo tanto de origen como de destino, además un dato adicional se debe especificar el tipo de mensaje NHRP. (Ortiz Palomino & López Cadena, 2019)

Tipos de mensajes proporcionados por el protocolo NHRP:

- Registro
- Resolución
- Redirección
- Purga
- Error

2.5. PROTOCOLO VRRP

VRRP, hace referencia al protocolo de redundancia de enrutador virtual, este protocolo está dirigido específicamente para la versión 3 de IPv4 e IPv6, cabe tener en cuenta que este protocolo brinda alta disponibilidad y redundancia en la red. (Orueta Diaz, San Cristobal Ruiz, Castro Gil, & Hernandez Berlinches, 2014)

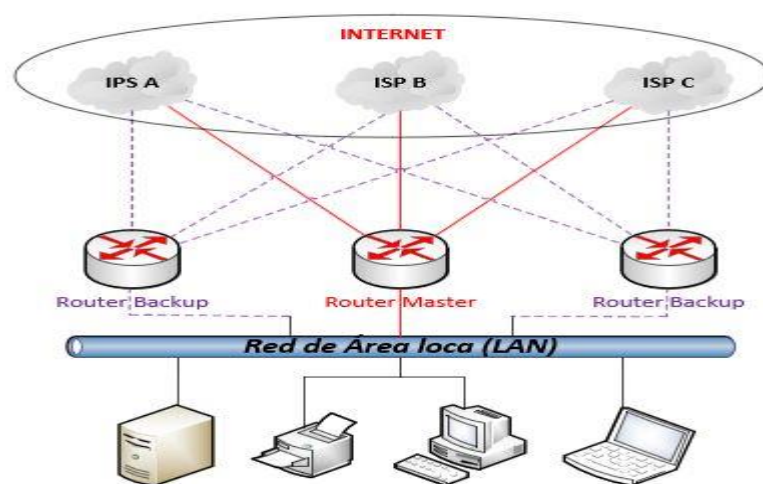
Cabe destacar que, al ofrecer redundancia en puntos estratégicos finales dentro de una red, es un deber crucial debido a que se puede configurar de una forma simple mediante VRRP, además tal cual como se lo exhibe en la figura 5, este protocolo brinda la opción de aumentar varios enrutadores virtuales en la topología para presentar una técnica más optima de recuperación de datos en la red siempre y cuando exista un fallo en la conectividad para un enrutador físico, por ejemplo que la conexión entre el router de la matriz y sucursal, se caiga la red, justo en ese momento el router backup el mismo que está bajo la configuración del protocolo backup, entra en operación para la redundancia de datos y evitar de esa manera que conectividad se pierda por completo. (Orueta Diaz, San Cristobal Ruiz, Castro Gil, & Hernandez Berlinches, 2014)

2.5.1. Funcionamiento de VRRP

VRRP, está bajo la definición de RFC 2338 el mismo que cumple con el siguiente funcionamiento:

- Este protocolo proporciona una dirección IP compartida y a la vez redundante dentro de un grupo de routers, en el cual está el denominado máster el mismo que tiene mayor prioridad en el grupo de routers mientras que los demás reciben el nombre de backup. (Orueta Diaz, San Cristobal Ruiz, Castro Gil, & Hernandez Berlinches, 2014)
- La MAC virtual trabaja bajo la configuración o en definitiva dentro del formato 0000.5e00.01xx, el cual xx representa el número de grupo en formato hexadecimal. Los hello de VRRP son enviados cada 1 segundo. (Orueta Diaz, San Cristobal Ruiz, Castro Gil, & Hernandez Berlinches, 2014)
- De forma predeterminada los routers o el grupo de routers involucrados que están bajo la configuración del protocolo VRRP toman el rol de máster en cualquier momento. (Orueta Diaz, San Cristobal Ruiz, Castro Gil, & Hernandez Berlinches, 2014)

figura 5. Topología del funcionamiento del protocolo VRRP



Elaborado por: Cristian Ibañez, Juan Pazmiño

2.6. EQUIPOS MIKROTIK

Equipos Mikrotik se trata de un producto el cual opera en una variedad de óptimos modelos los mismos que nos brinda la opción de efectuar una serie de múltiples

procedimientos a nivel de redes empresariales ya que ayudan a enfocarse en puntos estratégicos de red tanto a nivel administrativo como productivo, Mikrotik RouterOS es aquel sistema operativo del dispositivo físico routerboard, routerOS es un sistema operativo independiente sobre la base del Kernel Linux v2.6, ofrece una instalación rápida y fácil manejo en la utilización de su interfaz. Este producto cuenta con una alta gama de modelos los mismos que dependen de la intensidad de operación y solución en redes de la empresa a implementar. (MikroTik Company, 2019)

En los equipos Mikrotik existen dos tipos de intervenciones los cuales ayudan a tener un alto nivel de control tanto a nivel de seguridad como de servicio, los cuales son:

- **Control de seguridad:** Este control tiene como característica principal el brindar varias sucursales o en definitiva varias redes mediante VPN, así mismo el poder asociarse mediante una PC o laptop como si estuviera operando dentro de ella desde cualquier punto estratégico, en definitiva, tiene la finalidad de acceder a varios recursos con un alto nivel de seguridad. Este control tiene un alto porcentaje en seguridad mediante túneles L2TP/PPTP además cabe recalcar que tiene encriptación superior con IPSEC el cual brinda todo el nivel de privacidad adecuado. (MikroTik Company, 2019)

- **Control de calidad de servicio:** Este tipo de control opera justamente cuando el acceso a internet tiene dificultades en la velocidad de envío de datos, el cual se produce por una mala administración en la navegación que se encuentra bajo sitios importantes los mismos que son útiles para la carga y descarga de archivos tales como, ftp, p2p o VoIP, todos estos protocolos tienen la misma prioridad, con este tipo de control se pretende racionalizar y priorizar de una forma un poco más estratégica el ancho de banda dando priorización a aplicaciones en un orden específico tal cual lo son las aplicaciones interactivas, VoIP, navegación, correo electrónico, etc. (MikroTik Company, 2019)

CAPÍTULO 3

LÍNEA BASE DE LA INFRAESTRUCTURA DE LA RED DE PUNTONET S.A

3.1. EMPRESA PUNTONET S.A.

Preparación y Planificación

PuntoNet S.A. es una de las empresas proveedoras de servicio tales como, banda ancha, fibra óptica, centro de datos, tecnología empresarial y sistemas satelitales los mismos que son de alta calidad, cabe destacar que dicha empresa presta sus servicios a clientes representativos tales como: (PuntoNet, 2019)

- Banco Pichincha S.A.
- Claro S.A.
- Telefónica S.A.
- Cooperativa JEP S.A
- CNT S.A.
- Corporación Favorita S.A
- Aresa S.A.
- SRI.

Por consiguiente, se da a conocer la misión y visión de la empresa PuntoNet S.A.

- **Misión:** Trabajar en ser la empresa líder en oferta de soluciones tecnológicas. (PuntoNet, 2019)
- **Visión:** Ser una empresa con cultura de calidad, procesos efectivos, innovadas plataforma tecnológicas y colaboradores con certificaciones técnicas, comprometidos en satisfacer las necesidades integrales de telecomunicaciones, manteniendo la fidelidad de nuestros clientes PuntoNet. (PuntoNet, 2019)

Los sistemas de seguridad que implementa PuntoNet como empresa son de un alto nivel tanto en calidad como calidez, tales como: (PuntoNet, 2019)

- FORTINET
- CHECK POINT

- PALOALTO NETWORKS

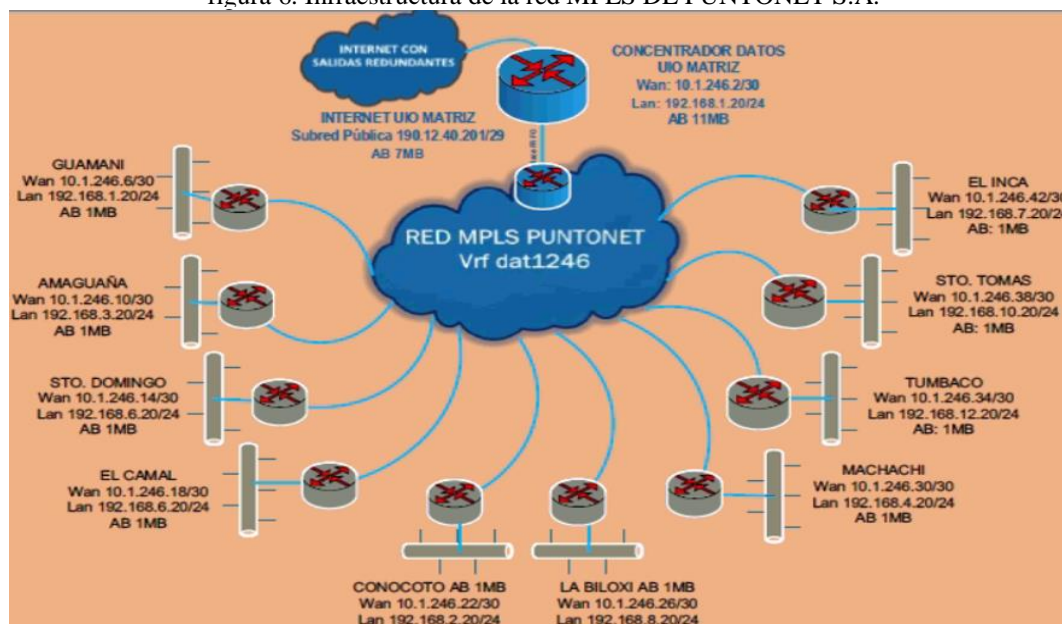
3.2. DESCRIPCIÓN DE LA INFRAESTRUCTURA DE LA RED PROVISTA POR PUNTONET A ESCALA NACIONAL

La empresa PuntoNet a una escala nacional cuenta en su infraestructura con 12 sucursales las mismas que están distribuidas en varias ciudades del país tales como; Ambato, Cuenca, El Coca, Guayaquil, Ibarra, Loja, Machala, Manta, Portoviejo, Quito, Riobamba y Santo Domingo, cabe destacar que cada una de las sucursales nombradas cuenta con su propio servidor así como una red de datos, voz y video, un dato adicional es que cada una operan o en definitiva están formalizadas sobre la red MPLS de PuntoNet. (PuntoNet, 2019)

3.2.1. La red MPLS de PuntoNet.

Como se lo exhibe en la figura 6 se muestra la distribución de la red MPLS de PuntoNet, como tal fue implementada a niveles de WAN, la misma que brinda la oportunidad de establecer una conexión a las distintas redes LAN existentes, atribuyendo que estas operan en el distrito metropolitano de Quito, respectivamente estas son aplicadas dentro de un rango, que abarca desde el concentrador de datos la matriz norte situada en el sector Iñaquito hacia la sucursal sur situada en el sector la Villa Flora. (PuntoNet, 2019)

figura 6. Infraestructura de la red MPLS DE PUNTONET S.A.



(PuntoNet, 2019)

3.3. ESTRUCTURA DE RED DE LA SUCURSAL SUR PUNTONET

La estructura de red en la que opera la sucursal sur presenta redundancia en lo que respecta a su última milla cabe mencionar que es un enlace fundamental o en definitiva principal, así como el backup están dispuestos y enfocados sobre la tecnología de fibra óptica PPP (Point to Point Protocol), además de contar con GPON (Gigabit Passive Optical Network), cabe destacar que este tipo de procesos y conjuntos tecnológicos otorga soporte como tal al tráfico de red en tiempo real en lo que respecta a la utilización de voz y video IP. (PuntoNet, 2019)

La infraestructura de la red sucursal sur se divide o se compone en dos términos esenciales tales como:

- **Red LAN:** Está compuesta por 3 pisos de operaciones o departamentos como se los conoce normalmente; atención al cliente, técnico y ventas masivas, existiendo un total de 26 usuarios por oficina sin descartar a la mano de obra técnica, cabe destacar que cada uno de los usuarios tienen acceso a la red mediante un equipo de borde denominado CE (Carrier Ethernet), la misma que se interconecta por la interfaz cliente. (PuntoNet, 2019)
- **Ancho de Banda:** Mediante una de sus interfaces se encuentra limitada entre los equipos de última milla tanto a nivel de capa 2 como de capa 3, el cual admite el abastecimiento de múltiples servicios otorgados por PuntoNet de manera simultánea, estos pueden ser servicios para la transmisión y recepción de datos, voz y video. (PuntoNet, 2019)

3.4. ESTRUCTURA DE RED DE LA MATRIZ PUNTONET.

La Matriz de PuntoNet cuenta con un Data Center el mismo que opera bajo la disponibilidad del estándar TIER III, este estándar se encuentra implementados o asociados en los siguientes equipos: (PuntoNet, 2019)

- CORE MPLS ASR 920
- Cisco serie Nexus
- NetApp (Sistema de almacenamiento de datos)
- OLT (Optical Line Termination), marca Calix E7-20

- OLT (Optical Line Termination), marca Core Access
- OLT (Optical Line Termination), marca ARBOR

Estos equipos son usados en si para atenuar ataques de seguridad a nivel de informática, un dato esencial es que estos equipos cuentan con redundancia el cual brinda una garantía de gran nivel para la continuidad del servicio de internet hacia los usuarios de las sucursales a escala nacional la misma que está basada en términos de redundancia geográfica, la cual abarca la interconexión de las ciudades de Quito y Guayaquil además esta provista mediante 3 proveedores que mediante conexión por fibra óptica, permiten la salida a nivel internacional. (PuntoNet, 2019)

Las conexiones internacionales son las siguientes:

- NAP de las Américas
- UFINET
- CW
- CNT
- NETFLIX
- FACEBOOK

La infraestructura de red de la matriz de PuntoNet está compuesta por:

- **Red LAN:** Esta red, está compuesta por las siguientes oficinas; atención al cliente, calidad y productividad, cobranzas, financiero, marketing, sistemas, supply chain, técnico, Gestión de talento humano, ventas masivas y corporativas, existiendo un total de 239 usuarios administrativos. (PuntoNet, 2019)

3.4.1. Especificaciones de los equipos físicos de PuntoNet

Central Telefónica IP

- Para la central telefónica en el cual consta el servidor de voz brinda o a su vez admite centralizar la comunicación desde la matriz hacia las demás sucursales a escala nacional, la aplicación de voz IP el cual se usa es Asterisk. (PuntoNet, 2019)

Equipos Core

- Estos equipos admiten el envío de información en lo que respecta desde la matriz hacia las demás sucursales ubicadas estratégicamente a escala nacional, la empresa de PuntoNet cuenta en su inventario con los siguientes equipos: (PuntoNet, 2019)

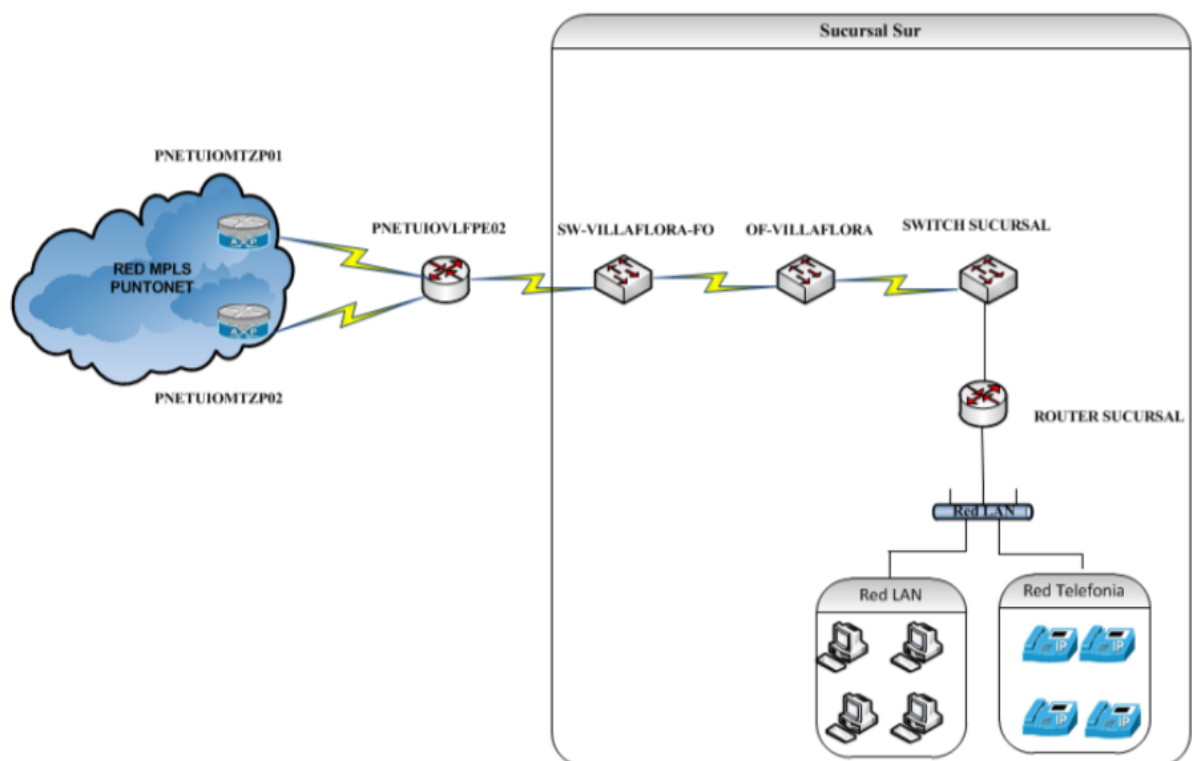
1. Equipos Cisco de la serie ASR 920 Y 9000
2. Equipos Mikrotik CCR 1072

Servidor

- Cuenta con el server PPPoE, el mismo que es esencial para la autenticación de usuarios además cabe destacar que es un protocolo de red que trabaja bajo la encapsulación PPP sobre una capa de ethernet. (PuntoNet, 2019)

Por consiguiente, como se puede observar en la figura 7, se exhibe el diagrama de la topología física de la red PuntoNet la cual refleja la forma en que se conectan la matriz hacia la sucursal sur.

figura 7. Diagrama físico de red Matriz-Sucursal Sur de PuntoNet.



(Manuel Araujo, 2019)

CAPÍTULO 4

DISEÑO DE LA RED MDVPN SOBRE LA RED MPLS DE PUNTONET

4.1. DISEÑO

Teniendo en cuenta los puntos trascendentales, de la línea base del proyecto, tanto a nivel técnico como de logística en lo que respecta a la interconexión o a su vez en la transmisión de datos entre la Matriz y Sucursal sur de PuntoNet, como siguiente punto principal se deriva en el diseño tomando en cuenta una estructura de red eficaz, es decir, que esta a su vez cuente con disponibilidad y escalabilidad en la red. El diseño de la infraestructura de la red MDVPN sobre la red MPLS de PuntoNet se basa en la descripción que existe en la interconexión de la Matriz y Sucursal sur de la empresa, encaminadas por una topología lógica y física respectivamente.

4.2. DISEÑO LÓGICO

En lo que corresponde al diseño lógico, se debe destacar que está basado en una arquitectura backbone, por ende, este admite la incorporación específica de un diseño lógico directamente virtual, es decir, como tal una topología virtual mediante routers IP los cuales operan sobre una topología física de conmutadores. Para la incorporación de este diseño lógico virtual, se hace uso del protocolo VRRP (Virtual Router Redundancy Protocol), como su nombre lo indica presenta redundancia en el caso de que llegase a presentarse algún tipo de fallo en el equipo maestro o matriz. Para ser más específico al momento de la configuración mediante el protocolo VRRP, en este caso se configura una IP virtual en los equipos a utilizar en este caso Mikrotik denominado para el diseño como backup, cabe mencionar que en esta configuración toca definir las IP virtuales como puertas de enlace para que de esta manera tenga mayor facilidad o a su vez acceso para el envío de paquetes y exista como tal la transmisión de información entre la Matriz y Sucursal Sur, este proceso se lo realiza mediante etiquetados los cuales brindan como tal las prioridades a la interfaz de cada uno de los equipos involucrados los mismos que estarán representados como matriz(hub) y sucursal (spoke) con la finalidad de que si en algún momento inoportuno en el envío de datos se pierde la conexión o servicio del equipo principal en este caso el equipo matriz(hub), el equipo con un etiquetado de menor prioridad en este caso backup, pasa a gestionar el servicio que estaba bajo la operación del equipo principal. Cabe mencionar que se hace uso del protocolo OSPF el cual admite elegir el camino

más corto para llegar al destino, además a nivel de seguridad en lo que respecta tanto la capa de red como la de transporte se utiliza el protocolo IPSEC (Internet Protocol security) e ISAKMP (Internet security association and key management protocol), el cual proporciona un alto nivel de mecanismo criptográfico, así como el implantar túneles seguros el cual permite la disponibilidad en la conexión de las redes LAN.

4.3. DIRECCIONAMIENTO IP

4.3.1. Direccionamiento de la red MPLS de PuntoNet

Tabla 1. Direccionamiento y asignación de puertos para red MPLS del equipo R1 de PuntoNet

Descripción	Red/ Dirección IP		Puerto asignado
Loopback	10.10.10.1		
R1-MPLS-R2	172.16.0.0/30	172.16.0.1/30	Ethe 2
R1-Matriz	172.16.0.20/30	172.16.0.21/30	Ethe 1

Elaborado por: Cristian Ibañez, Juan Pazmiño

Tabla 2. Direccionamiento y asignación de puertos para red MPLS del equipo R2 de PuntoNet

Descripción	Red/ Dirección IP		Puerto asignado
Loopback	10.10.10.2		
R2-MPLS-R1	172.16.0.0/30	172.16.0.2/30	Ethe 2
R2-SUCURSAL	172.16.0.28/30	172.16.0.30/30	Ethe 1

Elaborado por: Cristian Ibañez, Juan Pazmiño

Tabla 3. Direccionamiento y asignación de puertos para red MPLS del equipo R4 de PuntoNet

Descripción	Red/ Dirección IP		Puerto asignado
Loopback	10.10.10.4		
R4-MPLS-R2	172.16.0.12/30	172.16.0.13/30	Ethe 2
R4-BACKUP	172.16.0.60/30	172.16.0.62/30	Ethe 1

Elaborado por: Cristian Ibañez, Juan Pazmiño

4.3.2. Direccionamiento para la conexión de la matriz a la sucursal sur

En las tablas 4, 5 y 6, se da a conocer la asignación de puertos en cada uno de los equipos involucrados en la topología es situadas a los bridges los mismos que tienen como única finalidad en la interconexión de la red, así como la de ostentar la disponibilidad de transmitir los paquetes de la red como tal WAN y LAN.

Tabla 4. Direccionamiento IP y asignación de puerto para la conexión a la sucursal mediante el router R2

Descripción	Red/ Dirección IP		Puerto asignado
SUCURSAL	172.16.0.30/24	172.16.0.31/24	Ethe 1
Loopback	10.10.10.7		
Vrrp 1	192.168.3.0/24	192.168.3.15/24	

Elaborado por: Cristian Ibañez, Juan Pazmiño

Tabla 5. Direccionamiento IP y asignación de puerto para la conexión a la matriz mediante router R1

Descripción	Red/ Dirección IP		Puerto asignado
MATRIZ	172.16.0.28/24	172.16.0.29/24	Ethe 1
Loopback	10.10.10.5		
Vrrp 1	200.168.1.0/24	200.168.1.15/24	

Elaborado por: Cristian Ibañez, Juan Pazmiño

Tabla 6. Direccionamiento IP y asignación de puerto para la conexión al backup mediante router R4

Descripción	Red/ Dirección IP		Puerto asignado
BACKUP	172.16.0.60/24	172.16.0.61/24	Ethe 1
Loopback	10.10.10.8		
Vrrp 1	192.168.3.0/24	192.168.3.15/24	

Elaborado por: Cristian Ibañez, Juan Pazmiño

4.4. DISEÑO FÍSICO

Para el diseño e implementación de la topología física se la llevo a cabo mediante equipos de la marca Mikrotik mediante el modelo RB2011 IL-IN y RB 750, estos modelos disponen de dos tipos de puertos tales como fast Ethernet y gigabit Ethernet así como equipos CISCO 881-k9, los mismos que están ubicados a los extremos de la topología, siendo uno el router operativo de la matriz y el segundo como sucursal, cabe destacar que el enrutamiento se lo realizará mediante la utilización del protocolo de enrutamiento OSPF, el mismo que permitirá la conexión o a su vez la transmisión de información entre la Matriz y Sucursal Sur de PuntoNet. Como es de consideración para el previo diseño de la topología física, se hizo uso de los equipos Mikrotik y CISCO los cuales se exhiben en la tabla 7, cabe destacar que dichos equipos proporcionan una configuración de bajo nivel de dificultad lo que lo convierte en una tecnología amigable al momento de trabajar con la interfaz gráfica, las especificaciones técnicas de cada equipo se las exhibe como tal en los anexos, A, B y C.

Tabla 7. Descripción de equipos físicos

Marca/modelo	Total, de Equipos	Descripción del equipo
Cisco 881	2	MATRIZ Y SUCURSAL
Mikrotik RB 750	4	Red MPLS (IP DATOS MATRIZ R1, IP DATOS SUCURSAL R2, IP DATOS SUCURSAL R4)
Mikrotik RB 750	1	EQUIPOS backup
Mikrotik RB 2011	1	Switch de CONEXIÓN SUCURSAL SUR, BACKUP

Elaborado por: Cristian Ibañez, Juan Pazmiño

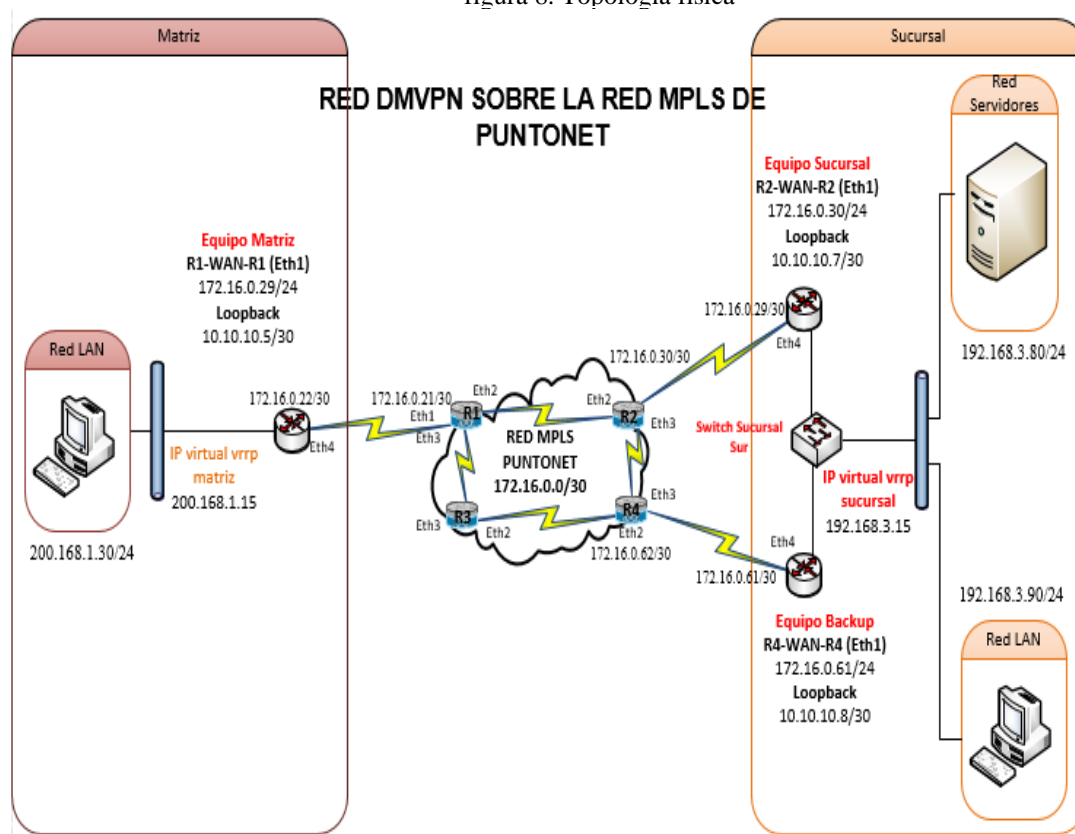
En la figura 8 se puede visualizar la distribución de los equipos de frontera los cuales están divididos por categoría o prioridad, es decir, los que trabajan tanto como máster y esclavos de la matriz y sucursal sur respectivamente.

La red MPLS está operando como un Router central el cual contiene en su configuración 4 equipos Mikrotik RB 750 como se especifica en la tabla 8, cabe

mencionar que el direccionamiento IP de la red MPLS se lo describe en las tablas previamente explicadas:

- Tabla 1: direccionamiento IP Router 1 red MPLS, Matriz
- Tabla 2: direccionamiento IP Router 2 red MPLS, sucursal sur
- Tabla 3: direccionamiento IP Router 4 red MPLS, backup

figura 8. Topología física



Elaborado por: Cristian Ibañez, Juan Pazmiño

4.5. IMPLEMENTACIÓN Y CONFIGURACIÓN

4.6. CONFIGURACIÓN Y PRIORIDAD PARA LA INTERFAZ LAN MEDIANTE EL PROTOCOLO VRRP

A continuación, se exhibe en la figura 9, las especificaciones de los comandos que se utilizó para la configuración, que se llevó a cabo, para el funcionamiento del protocolo vrrp en el equipo cisco denominado sucursal, además se exhiben en la figura 10, la tabla del protocolo VRRP resultante de dicha configuración.

figura 9. configuración del protocolo vrrp en la Sucursal, equipo cisco

Comando	Descripción
Interfaz vlan30	Se habilita el modo de configuración de la interfaz vlan30.
Vrrp 1 ip 192.168.3.15	Se asigna un Vrid el cual es un identificador de enrutamiento virtual, su rango va de 1 a 255, en este caso usaremos el Vrid=1, la dirección IP virtual asignada es la 192.168.3.15.
No vrrp 1 shutdown	Se habilita el enrutamiento virtual del protocolo vrrp en la interfaz.
Vrrp 1 source-ip 192.168.3.15	Este comando nos brinda determinar una dirección IP vrrp, pero de característica virtual la misma que se usara como una dirección IP de origen del envío de datos vrrp, esta dirección IP corresponde la sucursal IP LAN.
Vrrp 1 priority 200	Permite definir la prioridad del protocolo de redundancia el rango está establecido desde 1 a 255. En este caso determinamos una prioridad de 200.
Vrrp 1 timers advertise msec 1000	Activa el tiempo de mensajes sucesivos establecidos por el router principal vrrp, pero de características virtuales. En este caso se dispuso de un tiempo de 1000 segundos.

Elaborado por: Cristian Ibañez, Juan Pazmiño

figura 10. tabla del protocolo vrrp

```
SUCURSAL_1#sh vrrp
Vlan30 - Group 1
  State is Init
  Virtual IP address is 192.168.3.15
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 200
  Master Router is unknown, priority is unknown
  Master Advertisement interval is unknown
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En el caso de los equipos principales y backup que operan en la matriz y sucursal sur, se les asigna prioridades a las interfaces LAN, con la única finalidad de que operen respectivamente como equipo máster y esclavo, si es que en algún momento inoportuno la red o comunicación entre matriz(hub) y sucursal(spoke) falle. Con respecto a la configuración en el equipo Mikrotik, denominado como backup de igual manera ubicado en la sucursal sur se lo exhibe como tal en la figura 11, además aquí se asigna el valor con respecto a las prioridades en la que va a opera la interfaz LAN en el equipo Mikrotik RB750, en la sucursal sur de PuntoNet.

Aquí se la asigna la interfaz en este caso bridge 1, con la dirección IP 192.168.3.15, de la misma manera como en el equipo cisco se le proporciona un Vrid igual a 1, para que opere como identificador de enrutamiento virtual, se le proporciona la prioridad, además se determina el tiempo de conmutación, en este caso se ha colocado 5 segundos, en este caso el equipo Mikrotik, backup con menor prioridad toma el rol del equipo master generando redundancia en el enlace con un tiempo de conmutación de 5 segundos.

figura 11. Configuración para asignar la prioridad y tiempo de conmutación al protocolo VRRP en el equipo Mikrotik, backup

The screenshot shows the Mikrotik WinBox interface for configuring VRRP. The 'Interface <vrrp1>' window has the 'VRRP' tab selected. The configuration fields are: Interface: bridge1, VRID: 1, Priority: 80, and Interval: 5.00s. The 'Interval' field has a small 's' icon indicating seconds.

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se exhibe en la figura 12, queda configurado el protocolo VRRP mediante las consideraciones explicadas con anterioridad, así como su prioridad y tiempo de conmutación.

figura 12. Configuración protocolo VRRP equipo Backup

```
[admin@Backup_Sucursall] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
# NAME INTERFACE MAC-ADDRESS VRI PRI INTERVAL V V3..
0 RM vrrp1 bridge1 00:00:5E:00:01:01 1 80 5s 2 ipv4
[admin@Backup_Sucursall] >
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

4.7. CONFIGURACIÓN DMVPN

En primera instancia antes de proceder a la configuración en general, se hará en este punto una explicación detallada del proceso de configuración de la red MDVPN. Cabe mencionar que la tecnología DMVPN es propia de CISCO, con la finalidad de que sea usada a una gran escala en conexiones de nivel empresarial y su ves escalables, además solo se la puede configurar o en su defecto implementar en equipos con IOS quedando descartado su implementación en equipos ASAs.

Esta tecnología por configurar es muy importante debido a que combina en la creación de túneles GRE, con el protocolo de encriptación IPSec y el protocolo de resolución NHRP logrando así que nuestra red DMVPN cumpla con las expectativas de la empresa reduciendo en parte la carga administrativa. DMVPN ofrece además de una conexión segura entre la matriz y sucursal sur mediante la generación de túneles IPSec dinámicos, puede también implementar IP multicast, firewall y QoS.

Los componentes claves para la configuración de nuestra red MDVPN y los cuales forman parte de la tecnología CISCO DMVPN son los siguientes:

- NHRP
- IPSEC
- mGRE

Los dos primeros componentes como tal ya se explicaron en el capítulo 2, ahora nos centraremos en la explicación y funcionamiento del componente más importante para la conexión exitosa y a la vez funcional de nuestro diseño el mGRE.

El componente mGRE por sus siglas en inglés, multipoint generic Routing encapsulation, brinda o da paso a que una interfaz GRE soporte múltiples túneles generados por IPSEC. Cabe mencionar que mGRE para su funcionamiento requiere del protocolo NHRP.

- mGRE hace uso de una sola interfaz para todas las sucursales involucradas en la red, simplificando de esta manera la configuración de la red.
- Puede comunicar sucursales de forma directa, mediante la creación de un túnel bajo demanda virtual directo, es decir, ya no es necesario que el tráfico pase por la matriz como se hacía antes mediante el GRE.

En el anexo D, E y F se muestra la configuración DMVPN que se llevara a cabo la misma que está basada en 3 fases involucrando a los 3 componentes claves de la tecnología DMVPN además proporcionara una correcta comunicación entre la matriz y sucursal.

4.7.1. Configuraciones router principal matriz

4.7.2. Configuración del protocolo IPSEC (matriz)

Una vez determinadas y establecidas las direcciones IP propuestas en la topología física procedemos a la configuración del sistema de seguridad para el encriptado de los datos o paquetes que se enviarán en la red diseñada, como tal este sistema pertinente es el protocolo IPSEC. Como se lo explico previamente en el capítulo 2, IPSEC es un protocolo de seguridad a nivel de redes para sobreguarda los datos en la red, es decir, dispone integridad, autenticación y encriptación de datos, cabe destacar que este protocolo opera en la capa 3 del modelo OSI. Cabe mencionar que la configuración del protocolo de seguridad se lo llevo a cabo tanto en el equipo CISCO como Mikrotik, en el anexo G se puntualiza la configuración que se realizó en el equipo CISCO referente al protocolo ISAKMP.

Como se puede apreciar en las figuras 13 y 18, se hace uso primordial de los algoritmos ISAKMP, 3DES (triple Data Encryption Standard), AES (Advanced Encryption Standard) este algoritmo se encarga de brindar encriptación de una manera mucho más rápida así como delegando mejores longitudes de claves y SHA (Secure Hash Algorithm) este último algoritmo tiene como finalidad el autenticar todos los paquetes esto lo lleva a cabo mediante el uso de una clave compartida de 128 bits, debido a que estas técnicas de seguridad proporcionan a nuestro diseño de red, generación de claves, así como la mitigación de amenazas, encriptación y a su vez desencriptación de datos respectivamente, siendo factible y optimo ambos algoritmos al momento de mantener con integridad la información. En la configuración del IPSEC están presentes mediante fases, denominadas como fase 1 y 2 de negociación, las mismas que están explicadas en el capítulo 2.

Configuración del IPSEC equipo CISCO figura 13:

figura 13. configuración del protocolo IPSEC equipos CISCO

```
Router(config)#crypto isakmp policy 7
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#
Router(config-isakmp)#group 7
Router(config-isakmp)#
% Invalid input detected at '^' marker.
Router(config-isakmp)#group ?
  1  Diffie-Hellman group 1 (768 bit)
 14  Diffie-Hellman group 14 (2048 bit)
 15  Diffie-Hellman group 15 (3072 bit)
 16  Diffie-Hellman group 16 (4096 bit)
  2  Diffie-Hellman group 2 (1024 bit)
  5  Diffie-Hellman group 5 (1536 bit)
Router(config-isakmp)#group 5
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#lifetime 3600
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

- En primera instancia se procede a digitar el comando expuesto en la figura 14, dicho comando proporciona la definición en conjunto de parámetros que se utilizarán durante la negociación de políticas IKE (internet key exchange) en la fase 1, la política establecida en este caso es 7, cabe mencionar que el sistema IKE se encarga de crear una nueva política, dicha política se define mediante la prioridad numérica que va de un rango 1 a 10.000, teniendo en cuenta que la prioridad más alta es 1.

figura 14. Comando para la configuración del protocolo IPSEC

crypto isakmp policy 7

Elaborado por: Cristian Ibañez, Juan Pazmiño

- Como siguiente punto se digita el comando expuesto en la figura 15, en esta línea simplemente determinamos con que algoritmo criptográfico queremos trabajar, en tal caso se hace uso del 3DES (168-bit Triple DES).

figura 15. Comando para la configuración del protocolo IPSEC

encryption 3des

Elaborado por: Cristian Ibañez, Juan Pazmiño

- En esta línea se digita el comando expuesto en la figura 16, como su nombre lo indica se trata simplemente en la autenticación compartida, es decir, se basa específicamente en claves compartidas mediante el método de autenticación.

figura 16. Comando para la configuración del protocolo IPSEC

authentication pre-shared

Elaborado por: Cristian Ibañez, Juan Pazmiño

- En esta línea se digita el comando **group 5**, dicho comando se encarga de especificar el identificador de grupo proporcionado por Diffie-Hellman, en este caso se hizo uso del grupo 5 (1536 bit), en el anexo H se especifican los distintos grupos proporcionados por el protocolo Diffie-Hellman, después se procede a digitar el comando **lifetime 3600**, es simplemente para establecer el tiempo de vida de la SA (security association), cabe mencionar que el tiempo esta determinados en segundos.
- En esta línea se digita el comando expuesto en la figura 17, dicho comando tiene como finalidad el configurar una clave pre compartida de autenticación, en este caso nuestra clave será tesis, además en la dirección ubicamos una IP por defecto.

figura 17. Comando para la configuración del protocolo IPSEC

Crypto isakmp key tesis address 0.0.0.0

Elaborado por: Cristian Ibañez, Juan Pazmiño

configuración del IPSec equipo CISCO figura 18:

figura 18. configuración del protocolo IPSEC en equipos CISCO

```
Router(config)#crypto ipsec transform-set redes ah-sha-hmac esp-3des
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#mode transport
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#crypto isakmp policy 7
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#
Router(config-isakmp)#group 5
Router(config-isakmp)#
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#crypto isakmp key tesis address 0.0.0.0
A pre-shared key for address mask 0.0.0.0 0.0.0.0 already exists!
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

- Mediante esta línea de comando, expuesto en la figura 19, se establece un vínculo de transformación, es decir, es una composición tolerable de protocolos de seguridad y a su vez algoritmos que operaran en los routers de extremo a extremo, la clave a utilizar en esta transformación es redes, basándonos para esta configuración en el algoritmo criptográfico 3DES, además se establecen las políticas de seguridad que se utilizarán en la transferencia de datos, en este caso se eligió el modo transporte AH (Authentication Header), desde este punto se puede configurar la fase 2 de IPSEC.

figura 19. Comando para la configuración del protocolo IPSEC

Crypto ipsec transform-set redes ah-sha-hmac esp-3des

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se puede apreciar en la figura 20, se visualiza la configuración para establecer las políticas de seguridad del protocolo IPSEC al momento de enviar y recibir datos de extremo a extremo, se elige en este caso el modo transporte, encriptando la contraseña cisco.

figura 20. configuración de transformación de IPSEC profile y protección del túnel

```
Router(config)#
Router(config)#crypto ipsec transform-set redes ah-sha-hmac esp-3des
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#mode transport
Router(cfg-crypto-trans)#
Router(cfg-crypto-trans)#crypto ipsec profile cisco
Router(config)#
Router(config)#interface tunnel 1
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#tunnel protection ipsec profile cisco
Router(config-if)#
Feb  6 08:31:39.611: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

El comando expuesto en la figura 21, hace referencia al conjunto de transformaciones, es decir, nos indica que no es necesario la creación de un map crypto externo. Por último, nos indica que la seguridad mediante el algoritmo ISAKMP esta activa de extremo a extremo.

figura 21. Comando para la configuración del protocolo IPSEC

crypto ipsec profile

Elaborado por: Cristian Ibañez, Juan Pazmiño

4.7.3. Configuración del protocolo NHRP, OSPF y del túnel extremo a extremo (matriz)

En la figura tanto 22, como 23, se muestra la configuración de los túneles mediante el uso de los comandos del protocolo NHRP, cabe destacar que dichos comandos de este protocolo son añadidos bajo la interfaz del túnel, es decir, NHRP es de suma importancia para poder asociar la dirección IP de la interfaz del túnel del router de la sucursal, a la dirección IP de la interfaz física. El túnel para configurar se basa en mGRE (multipoint Generic Routing Encapsulation), con la finalidad de brindar a la red operaciones multipunto.

figura 22. configuración de los túneles dinámicos mediante el protocolo mGRE

Comando	Descripción
Interfaz tunnel 1	Se comienza a trabajar en el modo de configuración de interfaz.
direccion ip 172.16.10.30 255.255.255.252	Se activa la IP correspondiente brindándole así una dirección IP a la interfaz del túnel.
Tunnel source fastEthernet 1	Se habilita la fuente de salida del túnel en este caso lo hace mediante una fastethernet.
Tunnel mode gre multipoint	Se activa y da paso al túnel de encapsulación de enrutamiento genérico (GRE), con el cual podrá operar bajo el modo multipunto.
Ip nhrp network-id 7	Mediante este comando se activa el protocolo NHRP en la interfaz.
Ip nhrp map multicast Dynamic	Este comando tiene como finalidad exponer la lista de diferentes destinos que en defecto recibirá el tráfico generado por los datos enviados o transmitidos mediante el multicast y el broadcast.
Ip ospf network broadcast	Este comando se encarga de habilitar la configuración del protocolo OSPF para broadcast, esto se da debido a que OSPF al ser un protocolo de ruteo de estado de enlace y no genere inconvenientes en los extremos de la red.
Ip ospf priority	Este comando se encarga de disponer la prioridad, es decir, el router principal en este caso la matriz tomara la prioridad más alta como se indica en la configuración es de 255
Ip nhrp map multicast	Este comando se encarga de establecer la dirección IP para el túnel, así como el especificar los diferentes destinos que deben recibir paquetes tanto multicast como broadcast, este comando es esencial debido a que el protocolo OSPF requiere

Elaborado por: Cristian Ibañez, Juan Pazmiño

figura 23. Configuración del túnel mediante el protocolo NHRP (Matriz)

```
Router(config)#interface tunnel 2
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#ip nhrp map multicast dynamic
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#ip ospf network broadcast
Router(config-if)#
Router(config-if)#
Router(config-if)#ip ospf priority
Jun 10 12:47:22.439: %CDP-4-NATIVE_VLAN_MISMATCH: Native
Router(config-if)#ip os
Router(config-if)#ip ospf priority 255
Router(config-if)#exit
Router(config)#do wr
Building configuration...
[OK]
R2CISCO(config)#int
R2CISCO(config)#interface tun
R2CISCO(config)#interface tunnel 2
R2CISCO(config-if)#
R2CISCO(config-if)#ip nhrp map multicast
Jan 1 00:07:30.510: %CDP-4-NATIVE_VLAN_MISMATCH: Nati
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la figura 24, se exhibe la tabla del protocolo NHRP, en el cual se puede determinar la configuración para la creación de túneles dinámicos previamente explicada, además se muestra el OSPF con su prioridad, así como las políticas de seguridad ya establecidas en la red.

figura 24. Tabla del protocolo NHRP

```
crypto isakmp policy 7
  encr aes 256
  authentication pre-share
  group 5
crypto isakmp key tesis address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set tesis esp-aes
  mode transport
!
crypto ipsec profile DMVPN
  set transform-set tesis
!
!
!
!
!
interface Loopback0
  no ip address
  shutdown
!
!
interface Tunnel2
  ip address 172.16.10.29 255.255.255.0
  no ip redirects
  ip nhrp map multicast dynamic
  ip nhrp network-id 7
  ip nhrp redirect
  ip ospf network broadcast
  ip ospf priority 255
  tunnel source 172.16.0.29
  tunnel mode gre multipoint
  tunnel protection ipsec profile DMVPN
!
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

4.7.4. Configuraciones router sucursal

4.7.5. Configuración IPSEC Backup

figura 25. Funcionamiento del protocolo IPSEC en el equipo Mikrotik Backup

The screenshot shows the Mikrotik WinBox interface. The top part is a terminal window with the following content:

```
[admin@Backup_Sucursal] > ping 200.168.1.30
SEQ HOST                                SIZE TTL TIME  STATUS
0 200.168.1.30                          56 123 1ms
1 200.168.1.30                          56 123 0ms
2 200.168.1.30                          56 123 0ms
3 200.168.1.30                          56 123 0ms
4 200.168.1.30                          56 123 0ms
sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms
max-rtt=1ms

[admin@Backup_Sucursal] >
[admin@Backup_Sucursal] >
[admin@Backup_Sucursal] >
[admin@Backup_Sucursal] >
[admin@Backup_Sucursal] >
[admin@Backup_Sucursal] >
[admin@Backup_Sucursal] > ip
[admin@Backup_Sucursal] /ip> ipsec remote-peers
[admin@Backup_Sucursal] /ip ipsec remote-peers> pr
Flags: R - responder, N - natt-peer
# ID STATE
0 message-1-sent
[admin@Backup_Sucursal] /ip ipsec remote-peers>
[admin@Backup_Sucursal] /ip ipsec remote-peers>
```

The bottom part of the screenshot shows the IPsec configuration window. It has tabs for Policies, Groups, Peers, Remote Peers, Mode Configs, Proposals, Installed SAs, Keys, and Users. The 'Peers' tab is selected, showing a table with the following data:

#	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel	PH2 State
0	::/0		::/0		255 (...)	encrypt			
1	192.168.3.0/24		200.168.1.0/24		255 (...)	encrypt	require	yes	no phase2

Elaborado por: Cristian Ibañez, Juan Pazmiño

Configuración del IPSec equipo MIKROTIK Backup figura 25:

- ip ipsec peer, el cual me indica una conexión punto a punto teniendo en cuenta las direcciones por donde va a salir o entrar los datos. Además, en esta configuración se establece la negociación tanto de claves como algoritmos SA (security association), también se determina la clave en este caso tesis, en el puerto 500 (TCP/UDP), de la misma manera se establece un método de autenticación mediante el pre-shared, lo cual brindara una mayor seguridad cuando el Router Backup se levante.
- El comando ip ipsec proposal, esta línea tiene como finalidad el de establecer los datos propuestos los mismos que serán enviados mediante la técnica de seguridad IKE con ello se podrá establecer el SA para la gestión de políticas, la estructura de este comando se basa en añadir un sistema de autenticación de algoritmos, en la configuración, en este caso se hizo uso del predeterminado, auth-algorithms=sha1, se digita el método de encriptación el cual queremos que opere en nuestra red en este caso utilizamos el 3DES, enc-algorithms=3des, por ultimo ubicamos tanto la vida útil de operación como el

grupo de política en ambas configuraciones utilizando los valores predeterminados, lifetime=30m pfs-group=modp1024, (por defecto grupo 2).

4.7.6. Configuración del protocolo NHRP, OSPF y del túnel extremo a extremo (sucursal)

Como se exhibe en la figura 26, se exhibe la configuración de los protocolos NHRP, OSPF y de la creación de los túneles dinámicos extremo a extremo mediante el protocolo mGRE, la metodología de configuración es la misma que se llevó a cabo en el router matriz mediante las mismas especificaciones propuestas en la figura 22, teniendo en cuenta las direcciones IP, la clave para el router sucursal es la misma que se utilizó en el router matriz, a diferencia del router matriz en donde al OSPF se le estableció una prioridad de 255, en cambio al router sucursal se le determina la prioridad más baja en este caso 0.

figura 26. Tabla de configuración del protocolo NHRP y los túneles (sucursal)

```
crypto isakmp policy 7
  encr aes 256
  authentication pre-share
  group 5
crypto isakmp key tesis address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set tesis esp-aes
  mode transport
!
crypto ipsec profile DMVPN
  set transform-set tesis
!
!
!
!
!
!
interface Tunnel2
  ip address 172.16.10.30 255.255.255.252
  no ip redirects
  ip nhrp map 172.16.10.29 172.16.0.29
  ip nhrp map multicast 172.16.0.29
  ip nhrp network-id 7
  ip nhrp nhs 172.16.10.29
  ip nhrp shortcut
  ip ospf network broadcast
  ip ospf priority 0
  tunnel source 172.16.0.22
  tunnel mode gre multipoint
  tunnel protection ipsec profile DMVPN
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la siguiente figura 27, se hace referencia a la tabla del protocolo de enrutamiento OSPF, en el cual se muestra la configuración realizada en el router sucursal.

figura 27. Tabla configuración del protocolo OSPF (sucursal)

```
interface FastEthernet4
 ip address 172.16.0.22 255.255.255.252
 ip accounting output-packets
 duplex auto
 speed auto
 !
!
interface Vlan1
 no ip address
 !
!
interface Vlan30
 ip address 192.168.3.70 255.255.255.0
 ip accounting output-packets
 vrrp 1 ip 192.168.3.15
 vrrp 1 priority 200
 !
!
router ospf 1
 log-adjacency-changes
 network 172.16.0.20 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 200.168.1.0 0.0.0.255 area 0
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la figura 28, se exhibe la configuración del protocolo de enrutamiento OSPF, establecida en el equipo Mikrotik Backup, a diferencia de los equipos CISCO, el entorno de configuración de Mikrotik es un poco más amigable ya que, se lo hace de una manera gráfica en el cual solo se ingresa las direcciones IP establecidas como tal en el capítulo 4.

Otro punto importante para destacar en esta configuración es la asignación de envío de paquetes como tal de la misma manera que se hizo en los equipos CISCOS acá también se lo determina como broadcast, tanto para el bridge 1 como para la loopback, así como para la conexión a la WAN desde el R4 de la red MPLS hacia el router Backup.

figura 28. configuración del protocolo OSPF en el router Mikrotik backup

OSPF										
Interfaces	Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>										
Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area	Neig...	State	
DP Loopback	10	1	none	*****	broadcast	default	backbone	0	passive	
D R4_WAN_R4	10	1	none	*****	broadcast	default	backbone	1	designated ro...	
D bridge1	10	1	none	*****	broadcast	default	backbone	1	designated ro...	

OSPF										
Interfaces	Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>										
Name	Router ID	Running								
* default	0.0.0.0	yes								
ospf1	10.10.10.8	no								

OSPF										
Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>										
Network	Area									
10.10.10.8	backbone									
172.16.0.60/30	backbone									
192.168.3.0/24	backbone									
200.168.1.0/24	backbone									

OSPF										
Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>										
Area Name	Instance	Area ID	Type	Default C...	Interfac...	Active I...	Neighb...			
* backbone	default	0.0.0.0	default			3	3	2		

OSPF										
Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>										
Instance	Router ID	Address	Interface	State Changes						
default	10.10.10.4	172.16.0.62	R4_WAN_R4	5						
default	192.168.3.70	192.168.3.70	bridge1	4						

Elaborado por: Cristian Ibañez, Juan Pazmiño

CAPÍTULO 5

PRUEBAS Y ANÁLISIS DE CONECTIVIDAD DE LA RED DMVPN

5.1. RED DMVPN

Una vez determinada cada una de las configuraciones en los equipos propuestos en la topología física como se indica en la figura 8, y a la par explicadas detalladamente en el capítulo 4, se consigue finalizar con satisfacción el diseño de la red DMVPN sobre la red MPLS de Puntonet, mediante las pruebas y tablas de ruteo, consiguiendo una conexión estable y disponible entre la Matriz y sucursal sur de Puntonet.

5.2. PRUEBA Y ANÁLISIS DE COMUNICACIÓN EQUIPOS CISCO MATRIZ Y SUCURSAL

5.2.1. Tabla DMVPN matriz y sucursal

Como se puede apreciar en las figuras 29 y 30 se muestra la tabla DMVPN, matriz y sucursal respectivamente, en el cual se verifica las sesiones por decirlo de esa manera DMVPN las cuales se han determinado entre el router principal matriz y router de la sucursal.

En ambos routers de los extremos, es decir, matriz y sucursal, se confirma que esta creada la tunelización tanto de forma dinámica para el router matriz establecido por la letra D como estática para el router sucursal establecido por la letra S.

Por lo tanto, queda comprobado la creación y funcionalidad de los túneles dinámicos con éxito tanto en el router matriz (hub), como router sucursal (spoke).

figura 29. tabla DMVPN de la matriz

```
COM1 - PuTTY
ddr=172.16.0.22
Jun 17 13:18:50.579: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch detected on FastEthernet1 (10), with SUCURSAL1_FastEthernet2 (30).
Jun 17 13:19:05.087: %CRYPTO-4-IKMP_NO_SA: IKE message from 172.16.0.22 is not an initialization offer
MATRIZ#
MATRIZ#
MATRIZ#
MATRIZ#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding
UpDn Time --> Up or Down Time for a Tunnel
=====

Interface: Tunnel2, IPv4 NHRP Details
Type:Hub, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
1 172.16.0.22 172.16.10.30 UP 00:00:20 D
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

figura 30. figura 23. tabla DMVPN de la sucursal

```
SUCURSAL1#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding
UpDn Time --> Up or Down Time for a Tunnel
=====

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
1 172.16.0.29 172.16.10.29 UP 01:18:38 S
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la figura 31, se verifica la conexión exitosa del túnel de pares o por su denominación en inglés peer extremo a extremo mediante el protocolo NHRP, el cual demuestra que la comunicación y creación del túnel dinámico se dio sin ningún problema entre las direcciones IP 172.16.0.22 y 172.16.10.30.

figura 31. tabla de detalles del protocolo NHRP

```
COM1 - PuTTY
Interface: Tunnel2, IPv4 NHRP Details
Type:Hub, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
1 172.16.0.22 172.16.10.30 UP 00:00:20 D

MATRIZ#
Jun 17 13:19:50.579: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1 (10), with SUCURSAL1 FastEthernet2 (30).
Jun 17 13:20:50.579: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1 (10), with SUCURSAL1 FastEthernet2 (30).
Jun 17 13:21:50.579: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1 (10), with SUCURSAL1 FastEthernet2 (30).
MATRIZ#
MATRIZ#
MATRIZ#
MATRIZ#ping 172.16.10.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.30, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

5.2.2. Prueba de comunicación desde la matriz hacia la sucursal

figura 32. Tabla de enrutamiento IP

```
MATRIZ#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

10.0.0.0/32 is subnetted, 5 subnets
O    10.10.10.1 [110/21] via 172.16.0.30, 03:55:50, FastEthernet4
O    10.10.10.2 [110/11] via 172.16.0.30, 03:55:50, FastEthernet4
O    10.10.10.3 [110/31] via 172.16.0.30, 03:55:40, FastEthernet4
O    10.10.10.4 [110/41] via 172.16.0.30, 03:55:40, FastEthernet4
O    10.10.10.8 [110/51] via 172.16.0.30, 02:28:19, FastEthernet4
172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    172.16.0.0/30 [110/11] via 172.16.0.30, 03:55:51, FastEthernet4
O    172.16.0.4/30 [110/21] via 172.16.0.30, 03:55:51, FastEthernet4
O    172.16.0.12/30 [110/31] via 172.16.0.30, 03:55:41, FastEthernet4
O    172.16.0.20/30 [110/21] via 172.16.0.30, 03:55:51, FastEthernet4
C    172.16.0.28/30 is directly connected, FastEthernet4
L    172.16.0.29/32 is directly connected, FastEthernet4
O    172.16.0.60/30 [110/41] via 172.16.0.30, 02:28:31, FastEthernet4
C    172.16.10.0/24 is directly connected, Tunnel2
L    172.16.10.29/32 is directly connected, Tunnel2
O    192.168.3.0/24 [110/22] via 172.16.0.30, 00:20:48, FastEthernet4
200.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    200.168.1.0/24 is directly connected, Vlan10
L    200.168.1.15/32 is directly connected, Vlan10
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se puede visualizar en la figura 32, se despliega la tabla de enrutamiento IP, en el cual se verifica la conexión de rutas por el camino más corto mediante el protocolo de enrutamiento OSPF, así como la conexión directa mediante el túnel.

Mientras tanto en la figura 33, se puede observar la conexión exitosa entre la matriz y la sucursal, en el cual desde el router matriz se envía un ping a la dirección IP física del router Backup 172.16.0.61, siendo exitosa la comunicación, además se realiza otro ping desde la matriz pero esta vez a la dirección IP virtual del protocolo VRRP (LAN) de la sucursal, 192.168.3.15 y 192.168.3.60, dando como resultado una comunicación exitosa.

figura 33. ping desde la matriz hacia la IP física del Backup e IP virtual (LAN) de la sucursal

```
MATRIZ#ping 172.16.0.61
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.61, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
MATRIZ#ping 192.168.3.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.15, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
MATRIZ#ping 192.168.3.60
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.60, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

5.2.3. Tabla IPSEC

figura 34. tabla IPSec Matriz, conexiones activas de paquetes cifrados

```
MATRIZ#sh crypto engine connections active
Crypto Engine Connections
```

ID	Type	Algorithm	Encrypt	Decrypt	LastSeqN	IP-Address
33	IPsec	AES256+MD5	0	9007	9007	172.16.0.29
34	IPsec	AES256+MD5	9009	0	0	172.16.0.29
2016	IKE	MD5+AES256	0	0	0	172.16.0.29

Elaborado por: Cristian Ibañez, Juan Pazmiño

Mediante el comando **show crypto engine connections active**, como su nombre lo indica no permite visualizar las conexiones cifradas y descifradas que se encuentran activas, cabe mencionar que en la figura 34, se muestra los resultados de la fase 2 de negociación IKE, es decir, el total de paquetes cifrados y descifrados enviados además se determina que en este punto las security association (SA) durante el proceso de la fase 2 son unidireccionales por lo tanto se describe que cada security association (SA)

visualiza el estado de tráfico en una sola dirección, a continuación se puntualiza el envío de los 9.009 paquetes:

- **Los encriptados son salientes:** se tiene 9009 paquetes salientes cifrados en estado, en la dirección 172.16.0.29. mediante el algoritmo AES256+MD5.
- **Los descifrados son entrantes:** se tiene 9007 paquetes descifrados entrante a la dirección IP 172.16.0.29, mediante el algoritmo AES256+MD5, en el proceso de envío se tiene la pérdida de dos paquetes, los mismos que se justifican por estado físico de la topología, es decir, algún inconveniente en la conexión de los puertos.

En la figura 35, se visualiza que el estado del protocolo IPSec este activa, se muestra el túnel 2 encriptado el cual se genera entre la dirección IP 172.16.0.29 y 172.16.0.22 mediante el crypto map tag, el cual indica que el túnel creado, tiene acceso al puerto 500 (TCP/UDP).

- El total de paquetes encapsulados, encriptados y digeridos por el sistema de seguridad son 9009.
- Los paquetes desencapsulados, descryptados y verificados en total resultaron 9007 de un total 9009, como se puede apreciar la descripción nos indica **pkts compr Failed:0**, es decir no se verifica pérdidas en el envío de paquetes por lo que se justifica dicha pérdida como algún problema en la conexión física de los equipos por deterioro del cable UTP o conector RJ45.
- También se visualiza la configuración de transformación cabe destacar que mediante esta línea de comando configurada establece vínculos de transformación, es decir, es una composición de protocolos tanto de seguridad como algoritmos de cifrado y descifrado que están involucrados en la configuración previa de la red que operaran en los router de extremo a extremo, como se puede apreciar para esta configuración y análisis se optó por disponer del protocolo ESP (Encapsulating Security Payload), con una longitud de 256 bits hacia el algoritmo AES (Advanced Encryption Standard).

figura 35. tabla IPSec Matriz

```

MATRIZ#sh crypto ipsec sa
interface: Tunnel2
  Crypto map tag: Tunnel2-head-0, local addr 172.16.0.29

  protected vrf: (none)
  local ident (addr/mask/prot/port): (172.16.0.29/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.0.22/255.255.255.255/47/0)
  current peer 172.16.0.22 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9009, #pkts encrypt: 9009, #pkts digest: 9009
    #pkts decaps: 9007, #pkts decrypt: 9007, #pkts verify: 9007
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 172.16.0.29, remote crypto endpt.: 172.16.0.22
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet4
  current outbound spi: 0x920BE0BB(2450251963)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
    spi: 0x9C95FE34(2627075636)
      transform: esp-256-aes esp-md5-hmac ,
      in use settings = (Transport, )
      conn id: 33, flow_id: Onboard VPN:33, sibling_flags 80000006, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4484340/665)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE

```

Elaborado por: Cristian Ibañez, Juan Pazmiño

5.2.4. Tabla ISAKMP

figura 36. Tabla del protocolo ISAKMP Matriz

```

MATRIZ#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA

```

dst	src	state	conn-id	status
172.16.0.29	192.168.3.5	MM_NO_STATE	0	ACTIVE
172.16.0.29	172.16.0.22	QM_IDLE	2001	ACTIVE

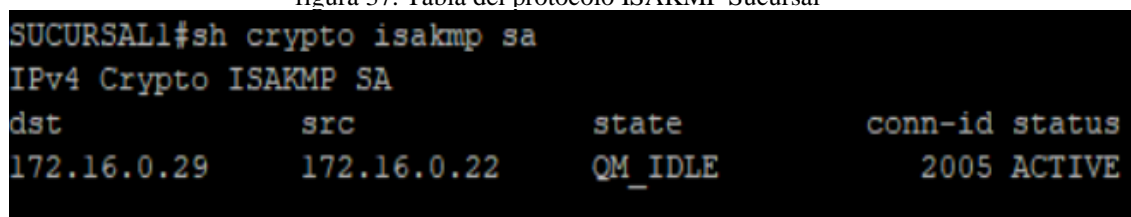
Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se puede apreciar en la figura 36, se exhibe como tal la tabla de security association (SA), del protocolo ISAKMP, el cual nos indica el estado de las negociaciones de seguridad, además verifica que la creación del túnel está habilitada o en su defecto se creó con éxito.

- **MM_NO_STATE:** Nos indica que el proceso del protocolo ISAKMP está activo, pero no ha continuado con la autenticación entre el túnel 172.16.0.29 a 192.168.3.5.
- **QM_IDLE:** en este estado nos indica que el protocolo ISAKMP se encuentra inactivo, pero a su vez está autenticando entre el túnel 172.16.0.29 a 172.16.0.22, es decir, a pesar de que está en estado inactivo, realiza la autenticación, como si estuviera activo.

En cambio, en la figura 37, se muestra la tabla del protocolo ISAKMP, pero de la sucursal, en el cual se observa que el estado de las negociaciones de seguridad se encuentra inactivo, pero está realizando la autenticación de paquetes.

figura 37. Tabla del protocolo ISAKMP Sucursal



dst	src	state	conn-id	status
172.16.0.29	172.16.0.22	QM_IDLE	2005	ACTIVE

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se puede observar en la figura 38, se muestra la tabla de sistema de seguridades de encriptación en el cual forma parte, security association (SA), en esta tabla se verifica el estado de seguridad de nuestra red, la vía de comunicación es mediante el túnel generado en la configuración previa del capítulo 4, el cual indica que está en estado activo mediante la dirección IP 172.16.0.22 en el puerto 500 (TCP/UDP), identificado en el proceso de configuración del IPSEC fase 1 de negociación SA. El sistema de administración de claves IKE SA, está habilitada mediante la dirección IP 172.16.0.29 correspondiente al router Matriz, remotamente conectado a la dirección IP 172.16.0.22. El protocolo IPSEC esta activado, permitiendo el paso de paquetes mediante la comunicación de las direcciones IP 172.6.0.29 y 172.16.0.22.

También se muestra que el estado de las negociaciones de security association (SA), están desactivadas pero en el puerto fastEthernet4, así como la conexión de pares o peer, en la dirección IP del router Backup de la sucursal 172.16.0.61, no está

identificado en las negociación SA, así mismo el sistema de administración de claves IKE SA, está inactiva en la comunicación 172.16.0.29 correspondiente al router Matriz, remotamente conectado a la dirección IP 172.16.0.61 del router Bachuk de la sucursal.

figura 38. Tabla del sistema de seguridad de encriptación IKE, IPSEC

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel2
Uptime: 00:01:04
Session status: UP-ACTIVE
Peer: 172.16.0.22 port 500 fvrf: (none) ivrf: (none)
  Phase1_id: 172.16.0.22
  Desc: (none)
  IKE SA: local 172.16.0.29/500 remote 172.16.0.22/500 Active
    Capabilities:(none) connid:2007 lifetime:00:58:54
  IPSEC FLOW: permit 47 host 172.16.0.29 host 172.16.0.22
    Active SAs: 2, origin: crypto map
    Inbound: #pkts dec'ed 1 drop 0 life (KB/Sec) 4452313/835
    Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4452313/835

Interface: FastEthernet4
Session status: DOWN-NEGOTIATING
Peer: 172.16.0.61 port 500 fvrf: (none) ivrf: (none)
  Desc: (none)
  Phase1_id: (none)
  IKE SA: local 172.16.0.29/500 remote 172.16.0.61/500 Inactive
    Capabilities:(none) connid:0 lifetime:0
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

5.3. PRUEBA Y ANÁLISIS EQUIPO MIKROTIK BACKUP, SUCURSAL

figura 39. Backup Down

```
Terminal
[admin@Backup_Sucursal] /interface vrrp> pr
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
#   NAME   INT.. MAC-ADDRESS      VRI PRI INTERVAL      V V3..
0   B vrrp1 bri.. 00:00:5E:00:01:01  1  80 1s              2 ipv4
[admin@Backup_Sucursal] /interface vrrp>
[admin@Backup_Sucursal] /interface vrrp> ..
[admin@Backup_Sucursal] /interface> ..
[admin@Backup_Sucursal] > ping 200.168.1.30
SEQ HOST                                SIZE TTL TIME   STATUS
0 200.168.1.30                          56 123 1ms   timeout
1 200.168.1.30                          56 123 0ms   timeout
2 200.168.1.30                          56 123 0ms   timeout
3 200.168.1.30                          56 123 0ms   timeout
4 200.168.1.30                          56 123 0ms   timeout
5 200.168.1.30                          56 123 0ms   timeout
6 200.168.1.30                          56 123 0ms   timeout
7 200.168.1.30                          56 123 0ms   timeout
sent=8 received=0 packet-loss=100%
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

figura 40. Backup up

```
Terminal
[admin@Backup_Sucursal] > interface vrrp
[admin@Backup_Sucursal] /interface vrrp> pr
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
#   NAME   INT.. MAC-ADDRESS      VRI PRI INTERVAL      V V3..
0   RM vrrp1 bri.. 00:00:5E:00:01:01  1  80 1s              2 ipv4
[admin@Backup_Sucursal] /interface vrrp> ..
[admin@Backup_Sucursal] /interface> ..
[admin@Backup_Sucursal] > ping 200.168.1.30
SEQ HOST                                SIZE TTL TIME   STATUS
0 200.168.1.30                          56 123 1ms
1 200.168.1.30                          56 123 0ms
2 200.168.1.30                          56 123 0ms
3 200.168.1.30                          56 123 0ms
4 200.168.1.30                          56 123 0ms
sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms
max-rtt=1ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En las figuras 34 y 40, se muestra la funcionalidad del router Backup como respaldo en el caso de existir algún fallo en la red, por ejemplo, en la figura 38 se ve que la red está funcionando correctamente por el cual el backup no realiza ningún trabajo de respaldo, se mantiene apagado o en Down. Mientras tanto en la figura 39 el backup se activa, es decir, toma el rol de equipo principal y se pone en modo UP, desde ese momento comienza a realizar el envío de datos, con un total de 123 saltos antes de llegar a su destino en un rango de 0 a 1 ms, teniendo en cuenta que el tiempo de

conmutación del router Backup una vez establecido como equipo principal es de 5 segundos.

5.3.1. Prueba de comunicación desde la sucursal hacia la matriz

Como se puede visualizar en la figura 41, se despliega la tabla de enrutamiento IP, en el cual se verifica la conexión de rutas por el camino más corto mediante el protocolo de enrutamiento OSPF, así como la conexión directa mediante el túnel.

figura 41. tabla de enrutamiento de la sucursal

```
SUCURSAL_1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

    10.0.0.0/32 is subnetted, 5 subnets
O       10.10.10.1 [110/11] via 172.16.0.21, 00:38:03, FastEthernet4
O       10.10.10.2 [110/21] via 172.16.0.21, 00:38:03, FastEthernet4
O       10.10.10.3 [110/21] via 172.16.0.21, 00:38:03, FastEthernet4
O       10.10.10.4 [110/31] via 172.16.0.21, 00:38:03, FastEthernet4
O       10.10.10.8 [110/41] via 172.16.0.21, 00:38:03, FastEthernet4
    172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.16.0.0/30 [110/11] via 172.16.0.21, 00:38:04, FastEthernet4
O       172.16.0.4/30 [110/11] via 172.16.0.21, 00:38:04, FastEthernet4
O       172.16.0.12/30 [110/21] via 172.16.0.21, 00:38:04, FastEthernet4
C       172.16.0.20/30 is directly connected, FastEthernet4
L       172.16.0.22/32 is directly connected, FastEthernet4
O       172.16.0.28/30 [110/21] via 172.16.0.21, 00:38:04, FastEthernet4
O       172.16.0.60/30 [110/31] via 172.16.0.21, 00:38:06, FastEthernet4
C       172.16.10.0/24 is directly connected, Tunnel2
L       172.16.10.30/32 is directly connected, Tunnel2
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, Vlan30
L       192.168.3.70/32 is directly connected, Vlan30
O       200.168.1.0/24 [110/22] via 172.16.0.21, 00:38:06, FastEthernet4
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En las figuras 42 y 43, se puede observar la conexión exitosa entre la sucursal y la matriz, en el cual desde el router sucursal se envía un ping a la dirección IP física del router matriz 172.16.0.22, siendo exitosa la comunicación, además se realiza otro ping desde la sucursal pero esta vez a la dirección IP virtual del protocolo vrrp (LAN) de la matriz, 200.168.1.15 y 192.168.3.60, dando como resultado una comunicación exitosa.

figura 42. Ping desde la sucursal a la IP virtual (LAN) de la Matriz

```
SUCURSAL1#ping 200.168.1.15

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.168.1.15, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
SUCURSAL1#ping 200.168.1.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.168.1.30, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

figura 43. Ping desde la sucursal a la WAN de la Matriz

```
SUCURSAL1#ping 172.16.0.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

5.4. VALIDACIÓN DE RETARDOS EN EL ENVIÓ DE PAQUETES

MATRIZ-SUCURSAL SUR

Para el análisis de tiempos de envío de paquetes se llevaron a cabo dos pruebas para la validación de retardos correspondiente al envío de 100 paquetes desde la matriz hacia la sucursal y viceversa, la primera prueba consta de un diseño con una configuración simple de una VPN estática en ambos extremos en cambio para su comparación la segunda prueba estará basada bajo la tecnología DMVPN.

Como se puede apreciar en la figura 44, se tiene el envío de 100 paquetes desde la matriz hacia la sucursal, la información es enviada hacia la dirección IP 192.168.3.90, en el cual se puede apreciar que el tiempo máximo que se demoró en llegar dicha información hacia el equipo sucursal es de 12 ms.

figura 44. Validación en el envío de paquetes desde la matriz hacia la sucursal bajo una configuración simple

```
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.168.3.90, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/12 ms
MATRIZ#ping 192.168.3.90 repeat 100 size 1500

Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.168.3.90, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/12 ms
MATRIZ#ping 192.168.3.90 repeat 100 size 1500
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la figura 45, se exhibe el envío de paquetes desde la sucursal hacia la matriz, de la misma manera que se hizo en la anterior prueba se hace el envío de 100 paquetes hacia la dirección IP, 20.168.1.30, donde se puede apreciar que el tiempo máximo en el cual los paquetes llegaron a su destino fue de 12 ms.

figura 45. Validación en el envío de paquetes desde la sucursal hacia la matriz bajo una configuración simple

```
Sucursal#ping 200.168.1.30 size 1500 repeat 100

Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 200.168.1.30, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/12 ms
Sucursal#ping 200.168.1.30 size 1500 repeat 100
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Una vez realizado lo que son las pruebas de envío de paquetes para la demostración de retardos en un escenario bajo la configuración de una VPN estática, se procede ahora a enviar los mismos 100 paquetes de matriz a sucursal y viceversa, pero esta vez mediante la configuración de la tecnología DMVPN en ambos routers para que de esta manera se pueda comprobar y en efecto comparar los tiempos de envío de datos.

En la figura 46, se puede apreciar el envío de paquetes desde la matriz hacia la sucursal, los 100 paquetes son enviados la dirección IP 192.168.3.90, en donde se exhibe que el tiempo máximo en el cual los paquetes llegaron a su destino fue de 4 ms.

figura 46. Validación en el envío de paquetes desde la matriz hacia la sucursal bajo una red con DMVPN

```

COM1 - PuTTY
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.168.3.90, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
MATRIZ#ping 192.168.3.90 repeat 100 size 1500

Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.168.3.90, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
MATRIZ#ping 192.168.3.90 repeat 100 size 1500

Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.168.3.90, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la figura 47, se puede apreciar el envío de paquetes desde la sucursal hacia la matriz, los 100 paquetes son enviados la dirección IP 200.168.1.30, en donde se exhibe que el tiempo máximo en el cual los paquetes llegaron a su destino fue de 4 ms.

figura 47. Validación en el envío de paquetes desde la sucursal hacia la matriz bajo una red con DMVPN

```

Sucursal#ping 200.168.1.30 size 1500 repeat 100

Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 200.168.1.30, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
Sucursal#ping 200.168.1.30 size 1500 repeat 100

Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 200.168.1.30, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

Elaborado por: Cristian Ibañez, Juan Pazmiño

En la tabla 8, se indica el tiempo en el cual cada paquete se demoró en llegar a su respectivo destino, teniendo como principal consideración que la red con DMVPN tuvo resultados favorables a comparación a la de una red con una configuración simple.

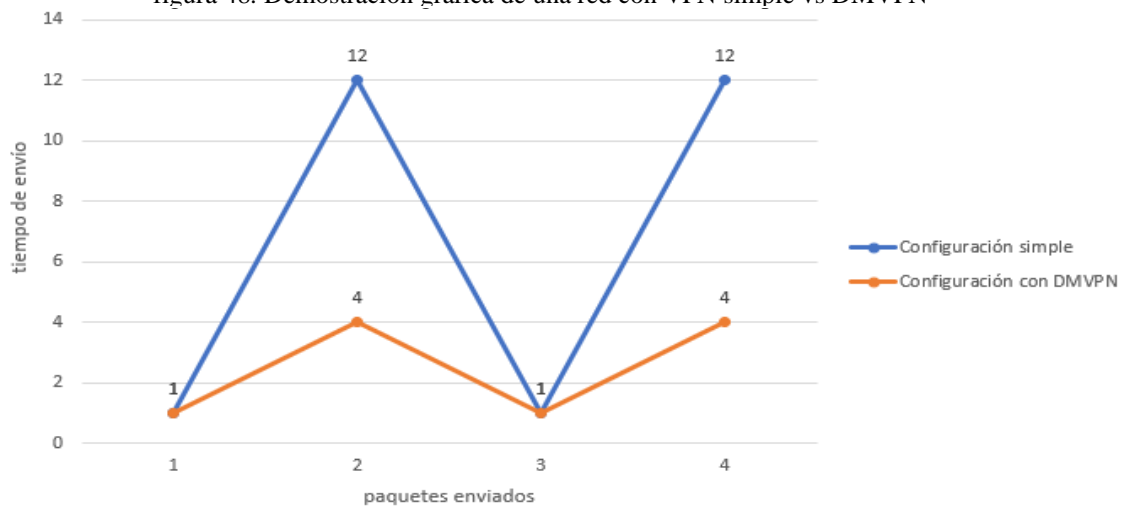
Tabla 8. Validación de retardos en el envío de paquetes Matriz-Sucursal

	Matriz-Sucursal		Sucursal-Matriz	
	Tiempo mínimo	Tiempo máximo	Tiempo mínimo	Tiempo máximo
Configuración simple	1 ms	12 ms	1 ms	12 ms
Configuración con DMVPN	1 ms	4 ms	4 ms	4 ms

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se exhibe en la figura 48, una vez realizado las pruebas previas con respecto al envío de paquetes, resulta que la tecnología DMVPN de una u otra manera facilita o en palabras más claras mejora el rendimiento de las interconexiones de redes a comparación de las pruebas que se realizaron al enviar paquetes a equipos en el cual la red DMVPN no está configurada, en tal caso se obtuvo un porcentaje considerable de mejora en el tiempo de llegada de paquetes a su destino en el cual la latencia se disminuyó un 70% o en definitiva el envío de paquetes hacia su destino disminuyo 8 ms. Cabe recalcar que DMVPN se sujeta en su configuración inicial a 3 términos esenciales, los cuales dan varios puntos a favor para un excelente rendimiento en el diseño propuesto tales como mGRE, NHRP e IPSEC.

figura 48. Demostración grafica de una red con VPN simple vs DMVPN



Elaborado por: Cristian Ibañez, Juan Pazmiño

IPSEC, es un protocolo que a pesar de ser un estándar de seguridad fundamental en la red DMVPN hace que el desempeño de la red disminuya, es decir, aumenta el retardo en el envío de paquetes, como se indica en el análisis previo, el proceso del protocolo

IPSEC es notable, debido a que al momento de realizar el tráfico de datos el proceso de encriptación toma tiempo el cual dio como resultado un retardo en la transmisión de paquetes de extremo a extremo, en el caso de una configuración simple se nota que el tiempo de 12 ms de llegado a su destino es muy considerable, mientras tanto al tratarse de una red configurada con tecnología DMVPN el protocolo IPSEC no afecta a gran escala su rendimiento, debido a que el tiempo máximo de llegado de los paquetes a su destino fue de 4 ms, a la par IPSEC es un sistema de seguridad de alto nivel, definido como flexible y a la vez potente, que ayuda a mantener la confidencialidad, integridad y autenticidad de los datos que son transmitidos dentro de la red.

Ahora se llevará a cabo la prueba de envío de paquetes desde el equipo matriz hacia el equipo backup, cabe recalcar que el equipo backup es tecnología Mikrotik por lo cual la configuración de una DMVPN en su sistema es imposible ya que dicha tecnología es propiedad de CISCO, solo para equipos con IOS.

Para dicha demostración se enviará un total de 100 paquetes de extremo a extremo, mediante el equipo Mikrotik, en la figura 49, se puede observar el envío de los 100 paquetes desde la matriz hacia la red LAN del equipo backup con la dirección IP, 192.168.3.90, se indica un tiempo máximo de llegado a su destino de 7 ms, además se puede observar cómo se realiza el proceso de negociación, encriptación y desencriptación de paquetes de extremo a extremo mediante el protocolo IPSEC en los routers de borde, desde la dirección IP, 172.16.0.61 hacia la IP, 172.16.0.22.

figura 49. Validación en el envío de paquetes desde equipo matriz hacia el equipo Backup prueba 1

```
[admin@Matriz_Prueba] > ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
0 E spi=0xBD9C15F src-address=172.16.0.61 dst-address=172.16.0.22
  state=mature auth-algorithm=sha1 enc-algorithm=aes-cbc
  enc-key-size=256
  auth-key="a87567053408e933479cf9b2b641bfe3deeebc86"
  enc-key="a0c2836fed102042ef3aa19282001714e9a18473dfe9a5977b01991f06
  6081ee"
  addtime=jan/15/1970 01:12:43 expires-in=8m4s add-lifetime=24m/30m
  current-bytes=10260 current-packets=171 replay=128
1 E spi=0x4FA530F src-address=172.16.0.22 dst-address=172.16.0.61
  state=mature auth-algorithm=sha1 enc-algorithm=aes-cbc
  enc-key-size=256
  auth-key="56ef601e19262a49d5136ca0a96c5e865b355ef3"
  enc-key="07f3b308222d3c7fc487ecfc428695751630e62936f069608e9d9a05dc
  a8ac39"
  addtime=jan/15/1970 01:12:43 expires-in=8m4s add-lifetime=24m/30m
  current-bytes=10260 current-packets=171 replay=128
[admin@Matriz_Prueba] >
```

SEQ	HOST	SIZE	TTL	TIME	STATU
80	192.168.3.90	1500	124	2ms	
81	192.168.3.90	1500	124	2ms	
82	192.168.3.90	1500	124	2ms	
83	192.168.3.90	1500	124	2ms	
84	192.168.3.90	1500	124	2ms	
85	192.168.3.90	1500	124	2ms	
86	192.168.3.90	1500	124	2ms	
87	192.168.3.90	1500	124	2ms	
88	192.168.3.90	1500	124	2ms	
89	192.168.3.90	1500	124	2ms	
90	192.168.3.90	1500	124	2ms	
91	192.168.3.90	1500	124	2ms	
92	192.168.3.90	1500	124	2ms	
93	192.168.3.90	1500	124	2ms	
94	192.168.3.90	1500	124	2ms	
95	192.168.3.90	1500	124	2ms	
96	192.168.3.90	1500	124	2ms	
97	192.168.3.90	1500	124	2ms	
98	192.168.3.90	1500	124	2ms	
99	192.168.3.90	1500	124	2ms	

```
sent=100 received=100 packet-loss=0% min-rtt=2ms avg-rtt=2ms
max-rtt=7ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se puede apreciar en la figura 50, se tiene el envío de 100 paquetes desde el equipo backup hacia la LAN del equipo matriz, en el equipo backup cabe recalcar que no está configurada por la tecnología DMVPN, los paquetes son enviados hacia la dirección del 200.168.1.30, como se puede observar se tiene un tiempo máximo de transmisión de datos de 2 ms, teniendo en cuenta que no hubo perdidas en el envío de paquetes, a diferencia del anterior envío de datos en este caso se puede observar el proceso de negociación, encriptación y desencriptación de paquetes de extremo a extremo mediante el protocolo IPSec en los routers de borde, desde la dirección IP, 172.16.0.22 hacia la IP, 172.16.0.61.

figura 50. Validación en el envío de paquetes desde el equipo Backup hacia el equipo matriz prueba 2

```
Terminal
[admin@Backup_Sucursall] > ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
0 E spi=0xE7D05AC src-address=172.16.0.22 dst-address=172.16.0.61
  state=mature auth-algorithm=sha1 enc-algorithm=aes-cbc
  enc-key-size=256
  auth-key="c1f3ec21d9ec60759dd4f0790f9cf6cadcd1c1f"
  enc-key="27568f8ec866b9398586b295c5c2df026cb9d0632354cef70d46439a14f0a9ad"
  addtime=feb/06/1970 01:58:30 expires-in=20m16s
  add-lifetime=24m/30m current-bytes=33060 current-packets=551
  replay=128
1 E spi=0x8CFF139 src-address=172.16.0.61 dst-address=172.16.0.22
  state=mature auth-algorithm=sha1 enc-algorithm=aes-cbc
  enc-key-size=256
  auth-key="2ef9e1ae0467924e6c87aeclde0724b2dfadc6cb"
  enc-key="1deff2533ffe7bc62bb488313b6f051ea0182238c4d99bd82dd45a88aefcf3769"
  addtime=feb/06/1970 01:58:30 expires-in=20m16s
  add-lifetime=24m/30m current-bytes=32760 current-packets=546
  replay=128
[admin@Backup_Sucursall] >

SEQ HOST                                SIZE TTL TIME STATUS
80 200.168.1.30                          1500 124 2ms
81 200.168.1.30                          1500 124 2ms
82 200.168.1.30                          1500 124 2ms
83 200.168.1.30                          1500 124 2ms
84 200.168.1.30                          1500 124 2ms
85 200.168.1.30                          1500 124 2ms
86 200.168.1.30                          1500 124 2ms
87 200.168.1.30                          1500 124 2ms
88 200.168.1.30                          1500 124 2ms
89 200.168.1.30                          1500 124 2ms
90 200.168.1.30                          1500 124 2ms
91 200.168.1.30                          1500 124 2ms
92 200.168.1.30                          1500 124 2ms
93 200.168.1.30                          1500 124 2ms
94 200.168.1.30                          1500 124 2ms
95 200.168.1.30                          1500 124 2ms
96 200.168.1.30                          1500 124 2ms
97 200.168.1.30                          1500 124 2ms
98 200.168.1.30                          1500 124 2ms
99 200.168.1.30                          1500 124 2ms
sent=100 received=100 packet-loss=0% min-rtt=2ms avg-rtt=2ms
max-rtt=2ms
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Tabla 9. Validación de retardo en el envío de paquetes Matriz-Backup

	Matriz (DMVPN)-Backup		Backup-Matriz (DMVPN)	
	Tiempo mínimo	Tiempo máximo	Tiempo mínimo	Tiempo máximo
Retardo en el envío de paquetes	1 ms	7 ms	2 ms	2 ms

Elaborado por: Cristian Ibañez, Juan Pazmiño

Como se puede notar en la tabla 9, existe una diferencia significativa en los tiempos al momento de enviar paquetes desde un equipo el cual tiene configurado DMVPN hacia uno que en efecto no la tiene, por ejemplo, cuando se enviaron paquetes desde el equipo matriz hacia el equipo Backup, el tiempo máximo de envío fue de 7 ms,

tomando en cuenta que en el equipo Backup no está configurado con DMVPN, en cambio al enviar los paquetes desde el equipo Backup hacia el equipo Matriz, la diferencia es notable ya que su tiempo máximo de transmisión de datos fue de 2 ms tomando en cuenta que en el equipo matriz está operando la tecnología DMVPN.

5.5. ANÁLISIS DE COSTOS PARA LA VIABILIDAD Y RENTABILIDAD DEL PROYECTO

Para la ejecución del proyecto propuesto y explicado cómo tal en el capítulo 4, es necesario realizar una evaluación a nivel económico para que de una u otra manera la empresa Puntonet pueda conocer el valor total de operación del proyecto en lo que implica tanto su rentabilidad, disponibilidad y viabilidad del diseño de la red DMVPN.

Para ello se tomará en cuenta el cálculo del VPN (valor presente neto) y TIR (tasa interna de retorno) con ello se podrá evaluar tanto del valor presente del costo de inversión como el de operación teniendo en cuenta los valores de mantenimiento y retiro de los equipos implementados en un futuro.

En la tabla 10, se detalla el costo tanto total como unitario de cada uno de los equipos implementados en el proyecto, así como el valor de mano de obra, cabe mencionar que en la topología física se muestra un solo switch, es decir, un equipo Mikrotik RB2011, pero se hizo uso de un segundo switch RB2011 para realizar las pruebas de conexión y funcionalidad solo para la red MPLS pero en si el equipo no es parte de nuestro diseño principal, en tal caso lo hemos tomado en cuenta para el análisis financiero de nuestro proyecto.

Tabla 10. Costo de equipos y materiales implementados en el proyecto

Marca/modelo	Cantidad	Costo unitario	Costo Total
Cisco 881	2	\$ 690.00	\$ 1,380.00
Mikrotik RB 750	5	\$ 100.00	\$ 500.00
Mikrotik RB 2011	2	\$ 200.00	\$ 400.00
Configuración de los equipos (mano de obra)			\$ 1,600.00
Subtotal			\$ 3,880.00
Iva 12%			\$ 465.60
total			\$ 4,345.60

Elaborado por: Cristian Ibañez, Juan Pazmiño

5.5.1. Cálculo del valor presente neto (vpn)

El cálculo del valor presente neto (VPN) es necesario para poder evaluar la viabilidad del proyecto para una futura implementación en el caso de que la empresa Puntonet lo desee, cabe destacar que el VPN es simplemente el resultado algebraico de traer al presente los flujos del proyecto utilizando una tasa de interés adecuada.

Para determinar el cálculo del VPN se hará uso de la fórmula que se muestra en la figura 51:

figura 51. Fórmula para el cálculo del valor presente neto (VPN)

$$VPN = -I_0 + R \left[\frac{1 - (1 + i/p)^{-np}}{i/p} \right]$$

Elaborado por: Cristian Ibañez, Juan Pazmiño

donde:

VPN: Valor presente neto

I_0 : Inversión inicial

R : Flujos del proyecto

i : Tasa de interés bancaria

p : Periodo de capitalización

n : periodos de operación

Para proseguir con el cálculo del VPN cabe mencionar que los valores con los cuales se llevara a cabo la evaluación de la viabilidad del proyecto son dotados y manejados por la empresa Puntonet como se puede apreciar en la tabla 11.

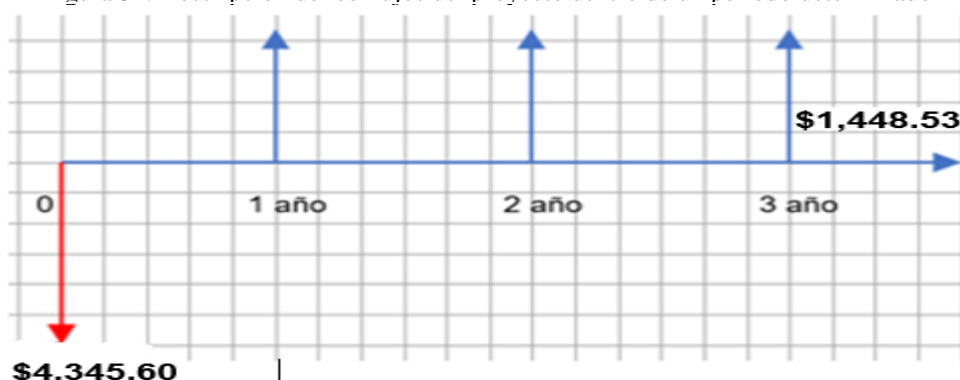
Tabla 11. Valores provistos por la empresa Puntonet para el cálculo correspondiente del VPN

Descripción	Valor
i: Tasa de interés bancaria	15%
n: periodos de operación vida útil de los equipos	3 años
R: Flujos del proyecto	\$1,448.53 por cada año de operación o vida útil de los equipos

Elaborado por: Cristian Ibañez, Juan Pazmiño

Cabe mencionar que los flujos de un proyecto de inversión son los movimientos del capital del proyecto que se dan en cada periodo para ello en la figura 52, hemos realizado un análisis del avance del proyecto durante los 3 años de vida útil de los equipos implementos teniendo en cuenta que el valor total calculado dispuesto en la tabla 11, es el capital o inversión inicial del año 0, y que los flujos del proyecto dentro de los 3 años de operación de la vida útil de los equipos es un valor proporcionado por la empresa Puntonet.

figura 52. Descripción de los flujos del proyecto dentro de un periodo determinado



Elaborado por: Cristian Ibañez, Juan Pazmiño

a. Evaluación año cero

$$VPN = \$ 4,345.60$$

b. Evaluación año 1

$$VPN = -4,345.60 + 1,448.53 * \left[\frac{1 - (1 + 0.15/1)^{-3(1)}}{0.15/1} \right] \quad \text{Ec. (5.1)}$$

$$VPN = -1,038.2873 \approx -\$1,038.29$$

c. Evaluación año 2

$$VPN = -4,345.60 + 1,448.53 * \left[\frac{1 - (1 + 0.15/2)^{-3(2)}}{0.15/2} \right] \quad \text{Ec. (5.2)}$$

$$VPN = 2,453.568 \approx \$ 2,453.57$$

d. Evaluación año 3

$$VPN = -4,345.60 + 1,448.53 * \left[\frac{1 - (1 + 0.15/3)^{-3(3)}}{0.15/3} \right] \quad \text{Ec. (5.3)}$$

$$VPN = 5,950.29 \approx \$ 5,950.30$$

El análisis referente a costos de inversión como se indica en los cálculos anteriores, el valor presente neto (VPN), en los 3 años de estudio del proyecto dio como resultado en el primer año de evaluación un valor menor a cero lo que indica que en el año 1 no se verán resultados del proyecto, mientras tanto que en los siguientes dos años de evaluación se tiene valores mayores a cero y por ende se generan ganancias por lo que da a entender que el proyecto es viable y en efecto puede ser implementado dando razón de que a la empresa Puntonet le conviene invertir en el proyecto.

5.5.2. Cálculo de la tasa interna de retorno (TIR)

La tasa interna de retorno (TIR) es aquella tasa la cual representa en interés con la que labora el proyecto de inversión además el valor presente neto en este cálculo es igual a cero, la fórmula para calcular el TIR se la exhibe en la figura 53.

figura 53. Fórmula para el cálculo de la tasa interna de retorno (TIR)

$$I_0 * (1 + TIR)^n = VPN_{total}$$

Elaborado por: Cristian Ibañez, Juan Pazmiño

donde:

TIR: tasa interna de retorno

VPN_{total} : valor presente neto total (la suma de los 3 años de flujo del proyecto)

I_0 : Inversión inicial

n : periodos de operación

$$4,345.60 * (1 + i)^3 = 7,365.58 \quad \text{Ec. (5.4)}$$

$$(1 + TIR)^3 = \frac{7,365.58}{4,345.60}$$

$$(1 + TIR) = \sqrt[3]{\frac{7,365.58}{4,345.60}}$$

$$TIR = 1.19230 - 1$$

$$TIR = 0.1923 \approx 19.23 \%$$

$$TIR = 19.23 \%$$

La tasa interna de retorno (TIR), dio como resultado 19.23%, siendo un valor mayor a la tasa de interés bancaria (i), que en este caso es del 15%, lo cual indica que mediante la realización de los cálculos pertinentes da como resultado que el proyecto es rentable, dichas demostraciones quedan justificados en la tabla 12.

Tabla 12. Descripción económica de la rentabilidad y viabilidad el proyecto

Términos	Descripción
VPN	<p>$VPN > 0$ (conviene invertir, genera ganancias)</p> <p>$VPN < 0$ (no conviene invertir, genera pérdidas)</p> <p>$VPN = 0$ (indiferente, no genera ganancias, ni perdida)</p>
TIR	<p>$TIR > i$ (rentabilidad conveniente para la empresa, es posible la aceptación del proyecto)</p> <p>$TIR \leq i$ (la rentabilidad no es conveniente para la empresa, es posible que rechacen el proyecto)</p>

Elaborado por: Cristian Ibañez, Juan Pazmiño

CONCLUSIONES

Con el diseño de la red DMVPN, se otorga mejoras en la conectividad empresarial entre matriz y sucursal al reducir la latencia un 70%, a comparación de realizar el envío de paquetes hacia equipos en el cual la red no está configurada con DMVPN, esta técnica de mejoramiento se da mediante la creación combinada de túneles dinámicos inteligentes con IPSec, generando una solución integral de seguridad para transferir datos sensibles sobre redes públicas sin afectar a los hosts individuales.

Al finalizar con las pruebas se puede corroborar que el protocolo de tunelización desarrollado por cisco mGRE con la implementación del protocolo de solicitud/respuesta de capa 2 NHRP permite que nuestra matriz (Hub) genere una base de datos con la dirección virtual y la dirección física de la sucursal (spoke) de forma automática cuando se enciende.

En base a las pruebas se puede determinar que el protocolo VRRP implementado entre los equipos de sucursal (CISCO) y el equipo backup (Mikrotik) ante una caída del equipo master el equipo esclavo (Mikrotik) con menor prioridad toma el rol del equipo master generando redundancia en el enlace con un tiempo de conmutación de 5 segundos.

Alusivo al análisis económico se concluye que el proyecto es rentable y a su vez viable ya que según los cálculos realizados con la implementación de equipos cisco y Mikrotik se garantiza la redundancia de la red, mitigando la latencia en las operaciones técnicas y operativas de la matriz y sucursal.

RECOMENDACIONES

Se sugiere revisar los IOS y versiones de los equipos cisco antes de generar cualquier configuración ya que si no son compatibles no se puede generar comunicación al igual que se debe actualizar fecha y hora en los equipos.

Es conveniente realizar un script en un documento de texto con las configuraciones que se debe realizar en equipos cisco para una configuración más ágil y rápida ya que si los comandos no son ingresados en el orden correcto la sesión del túnel no se levanta.

Se sugiere implementar equipos cisco de la serie 800 en adelante para futuras sucursales ya que los equipos Mikrotik no podrán ingresar a la base de datos MDVPN de la matriz ya que esta tecnología es propia de Cisco.

BIBLIOGRAFÍA

- Academy, C. N. (4 de febrero de 2020). *CISCO*. Obtenido de CISCO:
<https://www.cisco.com/c/en/us/support/routers/881-integrated-services-router-isr/model.html>
- Barrientos Sevilla, E., & Ariganello, E. (2015). *Redes Cisco: guía de estudio para la certificación CCNP Routing y Switching (3a. ed.)*. Madrid: RA-MA.
- Cisco Networking, A. (2014). *Switched Networks Companion Guide*. Indianapolis: Cisco Press.
- Dordoigne, J. (2020). *Redes informáticas nociones fundamentales (Protocolos, arquitectura, redes inalámbricas, virtualizacion, seguridad, IPV6) 7ma edición*. Barcelona: ENI.
- Edwin Antonio Mero, M., Ortiz Hernández, MSc, M. M., & Marcillo Parrales, MSc., K. G. (2019). *El Sistema de comunicación inalámbrico con tecnología Mikrotik para la transmisión de voz y datos Comunicación Inalambrica*. Manabí: Sinapsis.
- García, A. G. (2015). *UF1473 - Salvaguarda y seguridad de los datos*. Madrid: Elearning S.L.
- Ibañez, C., & Pazmiño, J. (27 de Noviembre de 2019). PuntoNet CAPACITACIÓN RED MPLS;. (I. L. Asnalema, Entrevistador)
- Maillo Fernandez, J. A. (2017). *Sistemas Seguros De Acceso y Transmisión de Datos*. Madrid: RA-MA.
- Manuel Araujo, L. V. (2019). *DISEÑO DE UNA RED SMART ROUTING SOBRE LA RED MPLS DE PUNTONET*. Quito: Politécnica Salesiana.
- MikroTik. (4 de Febrero de 2020). *MikroTik*. Obtenido de MikroTik:
<https://mikrotik.com/products>
- MikroTik Company. (Noviembre de 2019). *MikroTik*. Obtenido de MikroTik :
<https://mikrotik.com/aboutus>

Ortiz Palomino, V. R., & López Cadena, D. O. (2019). *Diseño de una red DMVPN SOBRE PROTOCOLO DE INTERNET VERSION 6 (IPV6) PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA*. Quito: UPS.

Orueta Diaz, G., San Cristobal Ruiz, E., Castro Gil, M. A., & Hernandez Berlinches, R. (2014). *Procesamiento y herramientas para la seguridad de redes*. Madrid: ISBN.

PuntoNet. (Noviembre de 2019). *PuntoNet Tecnología del mañana*. Obtenido de PuntoNet Tecnología del mañana: <https://www.puntonet.ec/>

Rubio, G. M. (2016). *QoS en routers y switches Cisco*. Lulu.

Tiso, J. (2014). *Interconnecting Cisco Network Devices, PART 2 (ICND2)*. Indianapolis: Cisco Press.

ANEXOS

Anexo A

Como se aprecia en la figura A, se dan a conocer las especificaciones técnicas del equipo Mikrotik RB750.

Figura A. Especificaciones técnicas equipo Mikrotik RB750

Product code	RB750UPr2
CPU nominal frequency	650 MHz
CPU core count	1
Size of RAM	64 MB
10/100 Ethernet ports	5
PoE in	Yes
Supported input voltage	6 - 30 V
Power output	On ports 2-5, Ourput: 1 A max per port; 2 A max total
PCB temperature monitor	Yes
Voltage monitor	Yes
Current monitor	Yes
USB slot	Yes
Dimensions	113 x 89 x 28 mm
License level	4
Operating System	RouterOS
CPU	QCA9531
Max Power consumption	51 W
Max power consumption without attachments	3 W

(MikroTik, 2020)

Anexo B

Como se aprecia en la figura B, se dan a conocer las especificaciones técnicas del equipo Mikrotik RB2011.

Figura A. especificaciones técnicas equipo Mikrotik RB2011

Model	RB2011iL		RB2011UiAS		
CPU	Atheros AR9344 600MHz				
Memory	64MB DDR SDRAM onboard memory		128MB DDR SDRAM onboard memory		
Ethernet	Five 10/100 Mbit Fast Ethernet ports with Auto-MDI/X Five 10/100/1000 Mbit Gigabit Ethernet ports with Auto-MDI/X				
Extras	Reset button, Reset jumper				
LEDs	Power, User, Ethernet activity				
Power input	Jack 8-28V DC; PoE in: 8-28V DC on Ether1 (Non 802.3af).				
Power output	500mA on Port 10				
Dimensions	Desktop:230x90x25mm Rackmount:443x92x44mm				
Power consumption	8W max		15W max		
Operating System	MikroTik RouterOS, L4 license		MikroTik RouterOS, L5 license		
Package includes	RB2011, power supply				

Feature / Model	2011iL-IN	2011iL-RM	2011iLS-IN	2011UiAS-IN	2011UiAS-RM
Enclosure	Desktop	Rackmount	Desktop	Desktop	Rackmount
SFP port	-	-	Yes	Yes	Yes
Power output	on port 10	on port 10	on port 10	on port 10	on port 10
USB	-	-	-	Yes	Yes

(MikroTik, 2020)

Anexo C

Como se aprecia en la figura C, se dan a conocer las especificaciones técnicas del equipo CISCO C881.

Figura C. especificaciones técnicas equipo cisco c881

Table 1 shows the Quick Specs.

Product Code	C881-K9
Rack Units	1RU
Interfaces	- LAN: 4 x 10Base-T/100Base-TX - RJ-45 - Management: 1 x console - RJ-45 - WAN : 1 x 10Base-T/100Base-TX - RJ-45 - USB : 1 x 4 PIN USB Type A
PoE	2 port integrated PoE
Performance Positioning	Up to 15 Mbps
RAM	256 (default) / 768 MB (Max)
Flash Memory	128 MB
Dimensions	32.5 cm x 24.9 cm x 4.4 cm
Package Weight	4.49 Kg

(Academy, 2020)

Anexo D

Como se puede observar en la figura D, se exhibe lo que es la configuración referente a la fase 1 del DMVPN, en el cual se complementa todo lo relacionado a la conexión de los equipos, es decir, desde la matriz hacia la sucursal y viceversa.

Figura D. Fase 1 de configuración del DMVPN, conectividad desde la matriz, hacia la sucursal.

```
matriz(config)#int tunnel 2 //aquí definimos el túnel para la matriz
matriz(config-if) #ip add 172.16.10.29 255.255.255.0
matriz(config-if) #tunnel source 172.16.0.29
matriz(config-if) #tunnel mode gre multipoint //activamos el mGRE
matriz(config-if) #ip nhrp network-id 7 //identificamos la conexión
matriz(config-if) #ip ospf net point-to-multipoint //identificamos la conexión
matriz(config-if) #tunnel protection ipsec profile DMVPN //activamos la protección del
túnel mediante el protocolo IPSec a la red DMVPN en la matriz
matriz(config-if) #exit

sucursal(config)#int tunnel 2 //aquí definimos el túnel para la matriz
sucursal(config-if) #ip add 172.16.10.30 255.255.255.252
sucursal(config-if) #ip nhrp network-id 7 //identificamos la conexión
sucursal(config-if) #ip ospf net point-to-multipoint
sucursal(config-if) #ip nhrp nhs 172.16.10.29
sucursal(config-if) #ip nhrp map 172.16.10.29 172.16.0.29
sucursal(config-if) #ip nhrp multicast 172.16.0.29
sucursal(config-if) #tunnel protection ipsec profile DMVPN //activamos la protección
del túnel mediante el protocolo IPSec a la red DMVPN en la sucursal
sucursal(config-if) #exit
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Anexo E:

Como se puede observar en la figura E, se exhibe la configuración referente a la fase 2 del DMVPN, en el cual se complementa la capacidad en la comunicación sucursal-sucursal, cabe destacar que en esta fase la sucursal remueve las direcciones de destino del túnel y se convierte en una interfaz mGRE, además determinan la dirección física de destino del túnel mediante el protocolo NHRP. La configuración de la matriz es el mismo que se realizó en la fase 1, también mostramos la configuración de OSPF.

Figura E. Fase 2 de configuración del MDVPN, optimización de comunicación sucursal-sucursal.

```
matriz(config-if) #ip nhrp map multicast dynamic
matriz(config-if) # ip ospf network broadcast
matriz(config-if) # ip ospf priority 255 //Dr (router designado), se usa para que los
intercambias de la LSU solo se realicen mediante el DR (matriz), en otras palabras,
los demás routers solo podrán intercambiar LSU con el router designado.

sucursal(config)#int tunnel 2 //aquí definimos el túnel para la matriz
sucursal(config-if) #ip add 172.16.10.30 255.255.255.252
sucursal(config-if) #tunnel source 172.16.0.29
sucursal(config-if) #tunnel mode gre multipoint //activamos el mGRE
sucursal(config-if) #ip nhrp network-id 7 //identificamos la conexión
sucursal(config-if) #ip nhrp nhs 172.16.10.29
sucursal(config-if) #ip nhrp map 172.16.10.29 172.16.0.29
sucursal(config-if) #ip nhrp multicast 172.16.0.29
sucursal(config-if) # ip ospf network broadcast
sucursal(config-if) # ip ospf priority 0 //Drother, solo se encargará de formar
adyacencias full con el DR.
sucursal(config-if) #tunnel protection ipsec profile DMVPN
sucursal(config-if) #exit
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Anexo F

Como se puede observar en la figura F, se exhibe la configuración referente a la fase 2 del DMVPN, en el cual se complementa la optimización de conectividad entre la matriz y sucursal, basado en el protocolo NHRP.

Figura F. Fase 3 de configuración del MDVPN, optimización de comunicación sucursal-sucursal.

```
matriz(config-if) #ip nhrp redirect //camino optimo, para alcanzar a otras sucursales
matriz(config-if) # exit

sucursal(config-if) # ip nhrp shortcut //permite a la sucursal realizar un proceso de
información de redirecciones desde la matriz.
sucursal(config-if) #exit
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Anexo G

Como se puede observar en la figura G, se exhibe la configuración referente al protocolo ISAKMP, el cual como se explicó con anterioridad en el capítulo 2, tiene como única finalidad la creación, intercambio y gestión autónoma tanto de claves como de autenticaciones, así como el trabajo de buscar cualquier tipo de amenaza que interrumpa como tal en la comunicación de la matriz y sucursal.

Figura G. configuración del protocolo ISAKMP

```
matriz(config)#crypto isakmp policy 7
matriz(config-isakmp) #encryption 3des 256
matriz(config-isakmp) #authentication pre-shared
matriz(config-isakmp) #group 5
matriz(config-isakmp) #lifetime 3600
matriz(config-isakmp) #exit
matriz(config)#crypto isakmp key tesis address 0.0.0.0
matriz(config)#crypto ipsec transform-set tesis ah-sha-hmac esp-3des
matriz(config-crypto-trans) #mode transport
matriz(config-crypto-trans) #exit

matriz(config) #crypto ipsec profile DMVPN
matriz(config) #tunnel protection ipsec profile DMVPN
matriz(ipsec-profile) #set transform-set tesis
matriz(ipsec-profile) # exit
```

Elaborado por: Cristian Ibañez, Juan Pazmiño

Anexo H

Como se aprecia en la figura H, se dan a conocer los distintos grupos existentes determinados por el protocolo de establecimiento de claves de pares o extremos.

Figura H. referencia de los grupos de Diffie-Hellman implementado por el protocolo IPSec

Referencia	Grupo	Nombre
RFC 2409	Group 1	768 bit MODP group
RFC 2409	Group 2	1024 bit MODP group
RFC 2409	Group 3	EC2N group (2^{155})
RFC 2409	Group 4	EC2N group (2^{185})
RFC 3526	Group 5	1536 bit MODP group
RFC 3526	Group 14	2048 bit MODP group
RFC 3526	Group 15	3072 bit MODP group
RFC 3526	Group 16	4096 bit MODP group
RFC 3526	Group 17	6144 bit MODP group
RFC 3526	Group 18	8192 bit MODP group
RFC 5903	Group 19	256 bits random ECP group
RFC 5903	Group 20	384 bits random ECP group
RFC 5903	Group 21	521 bits random ECP group

Elaborado por: Cristian Ibañez, Juan Pazmiño